Welcome to this Thesis Defense

Presented by MFOGO Volviane Saphir

HACKED

HACKED

HACKED

REPUBLIQUE DU CAMEROUN
PAIX - TRAVAIL – PATRIE
****
UNIVERSITE DE DSCHANG
****
ÉCOLE DOCTORALE

REPUBLIC OF CAMEROON
PEACE - WORK - FATHERLAND
****
UNIVERSITY OF DSCHANG
****
POST GRADUATE SCHOOL

DSCHANG SCHOOL OF SCIENCES AND TECHNOLOGY
RESEARCH UNIT IN FUNDAMENTAL COMPUTING, ENGINEERING AND APPLICATIONS (RUFCEA/URIFIA)

MACHINE LEARNING FOR CYBER DECEPTION IN INTERNET OF THINGS

PhD/Thesis Presented by

MFOGO Volviane Saphir
Registration number**: CM-UDS-14SCI2035**
Master in Mathematical Sciences

Under the supervision of:

Pr NKENLIFACK Marcellin
Full Professor
University of Dschang

Pr ZEMKOHO Alain
Full Professor
University of Southampton

Dr YAMEN NJILLA Laurent
Senior Research Engineer
Air Force Research Laboratory

April, 2025

The Mirai Botnet Attack (2016)

Table of Contents

- Introduction
  - Context
  - Problem
  - Objectives
- Literature Review
  - Detection
  - Honeypot
  - Deception
- Contributions & Results
  - Cyber Deception for Probing Attacks
  - Hybrid Recommender System Approach for Cyber Deception
  - Augmented Reality Honeypots
- Conclusion
  - Summary
  - Limitations
  - Future Works

Introduction

The 2024 Roku Cyberattack

What is a thing?

Smart Refrigerator

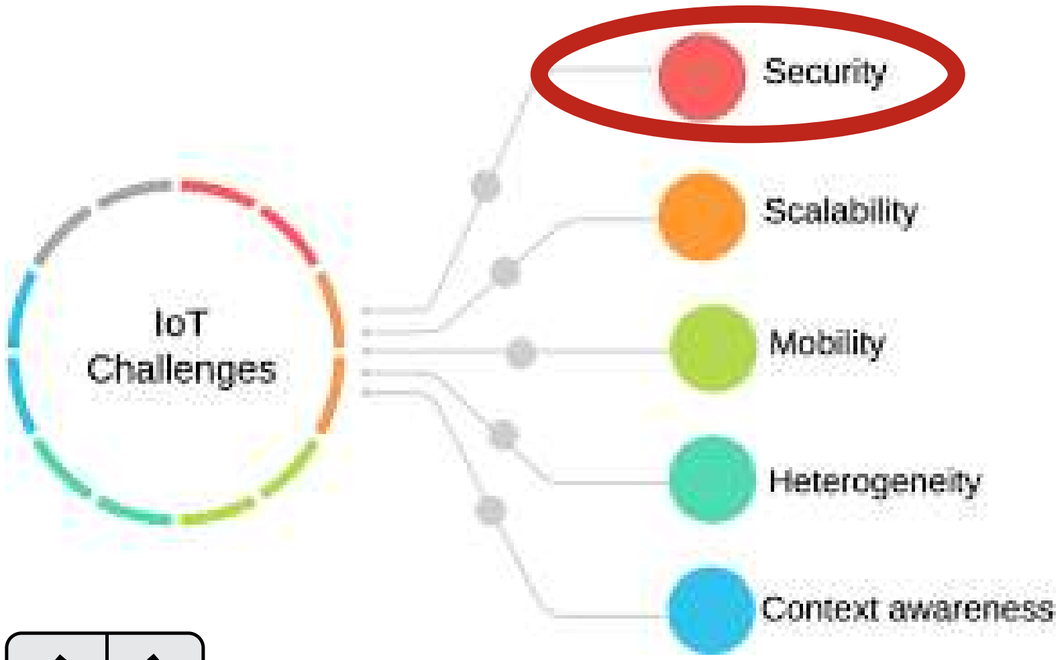
Smart Watch

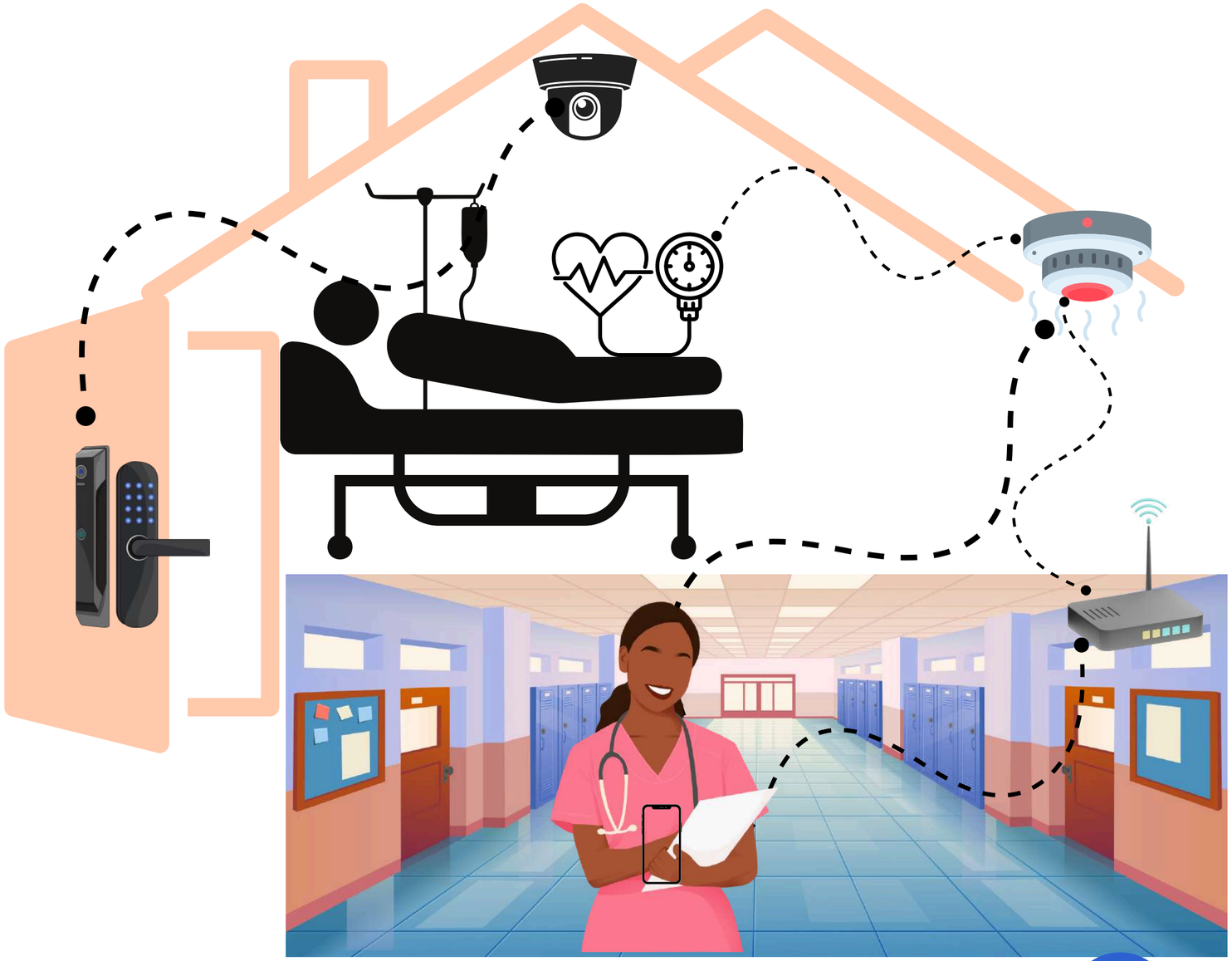
Smart Surveillance Camera

What is the Internet of Things?

IoT in Healthcare: A real-world scenario

- IoT Network in the Hospital
- Purpose of IoT Integration
- Security Challenge

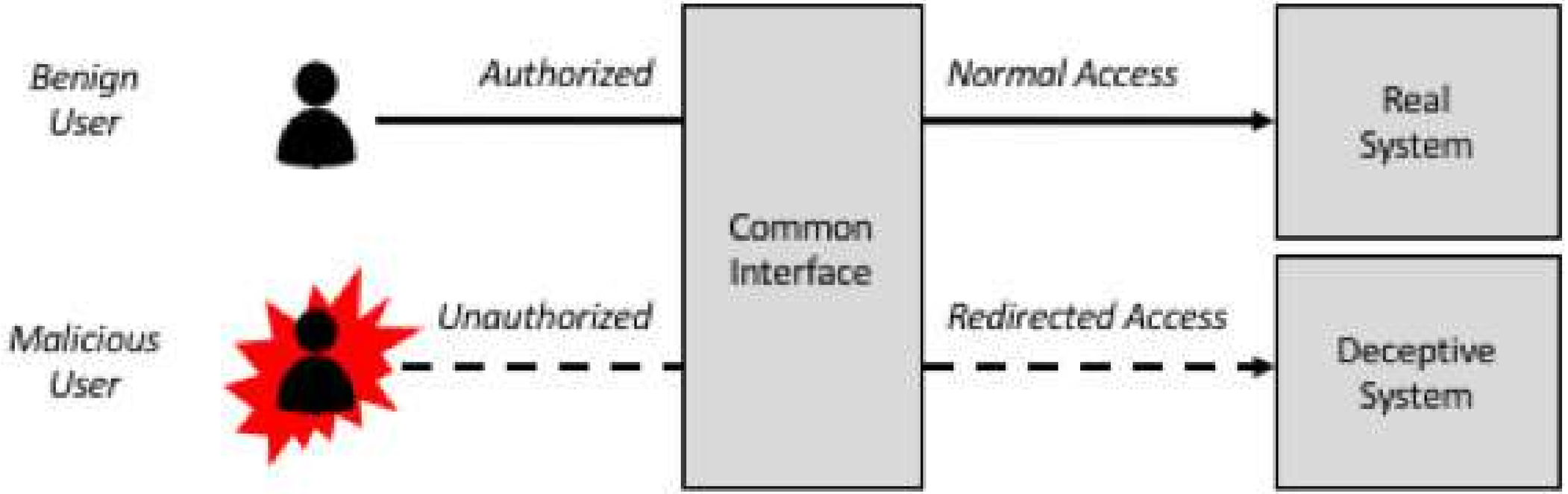




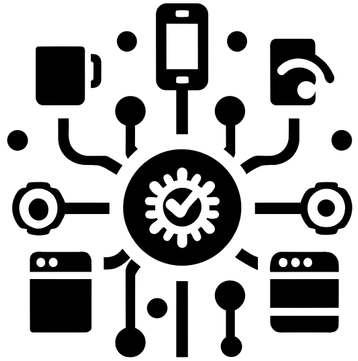
The context

- **Extensive Connectivity:** By 2025, it’s estimated that over 75 billion IoT devices will be connected worldwide.
- **Security Neglect:** A study found that 48% of companies using IoT devices have experienced a security breach. Additionally, 80% of IoT devices are vulnerable to attacks due to weak security measures.
- **Inadequate Traditional Solutions:** Traditional security solutions fail to protect against 60% of IoT-related cyber threats.
- **Growing Threats:** The number of IoT cyberattacks increased by 300% in 2019 alone, and this trend is expected to continue as more devices come online.

Inadequate Traditional Solutions =? Cyber Deception



Problems



The rapid proliferation of Internet of Things (IoT) devices

Grows Vulnerability

Existing Solutions are Reactive

Insufficient Existing Security Measures

Traditional IoT security relies on reactive mechanisms that address threats only after they have occurred. These approaches are inadequate against sophisticated, adaptive cyber threats targeting IoT systems.

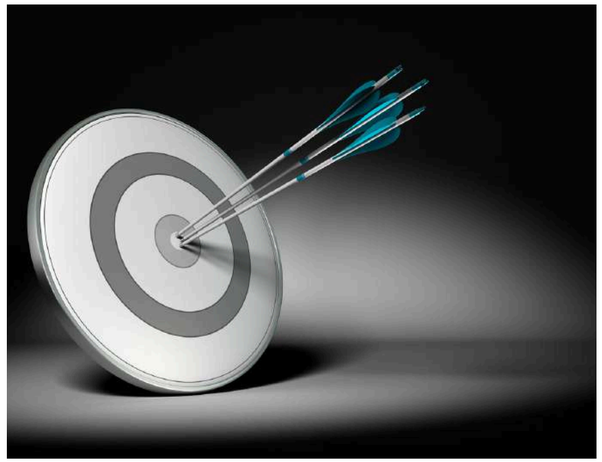
Urgent Need for Proactive Solutions

The evolving threat landscape highlights an urgent need for proactive security solutions that can anticipate, detect, and mitigate attacks before they occur, especially in high-stakes environments like healthcare.

Research Questions

- What are the common vulnerabilities in IoT devices, and how can they be exploited by attackers?
- What cyber deception techniques can be designed to effectively mislead and capture attackers?
- How can machine learning techniques be applied to detect and mitigate cyber threats targeting IoT devices?
- How can machine learning improve cyber deception in IoT?
- What are the benefits of using RL-based techniques for IoT security?
- How effective is cyber deception in IoT camera security?

General Objectives



OBJECTIVE : LITTERALY

Develop a proactive security measure capable of addressing the expansion of the number of devices and adapting to new types of sophisticated vulnerabilities and attacks.

OBJECTIVES: THECNICALLY

Develop a comprehensive security framework that integrates machine learning and cyber-deception techniques to protect IoT devices from cyber threats.

Specific Objectives

OBJECTIVE 01

To identify and analyze common vulnerabilities in IoT devices.

OBJECTIVES 02

To develop machine learning models for detecting cyber threats targeting IoT devices.

OBJECTIVES 03

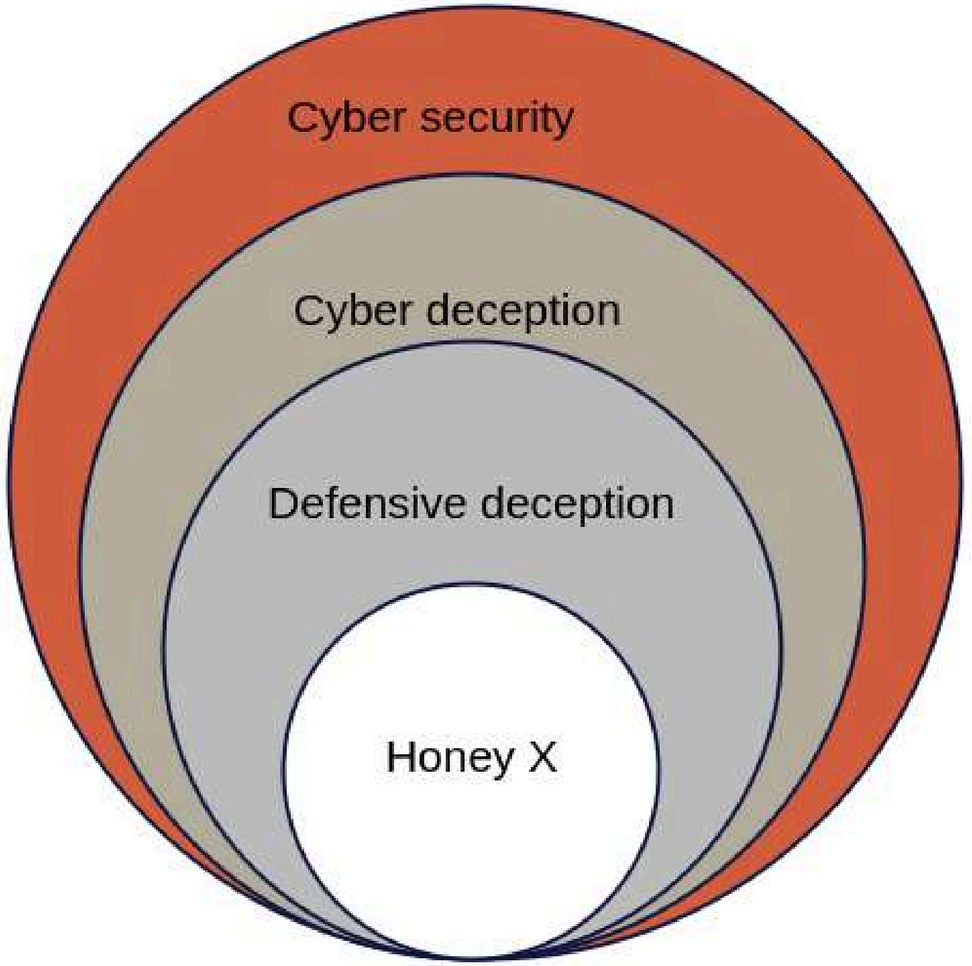
To design and implement cyber deception techniques for misleading and capturing attackers.

OBJECTIVES 04

To evaluate the effectiveness of the proposed security framework through simulations and real-world case studies.

Cyber deception

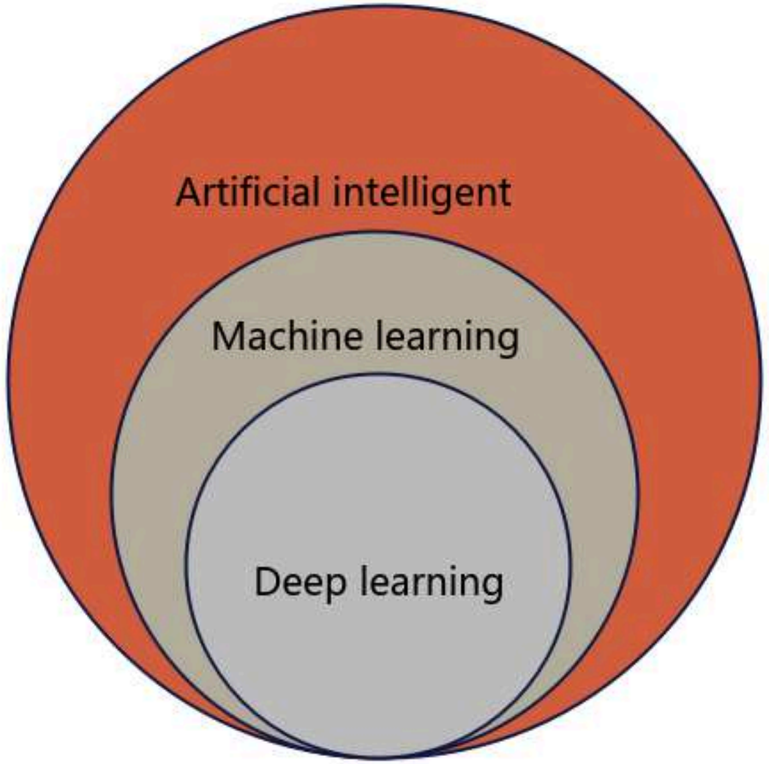
Cyber deception is a proactive cybersecurity strategy that involves creating a network of deceptive elements, such as decoys to mislead and divert potential attackers.



Cyber deception

- **Conceptual Deception Tactics:** Masking, Repackaging, Dazzling, Mimicking, Inventing, Decoying, Bait.
- **Expected Effects of Defensive Deception:** Hiding, Luring, Misleading, Blending, Confusing
- **The ultimate goals** are to protect assets or detect attackers

Machine Learning

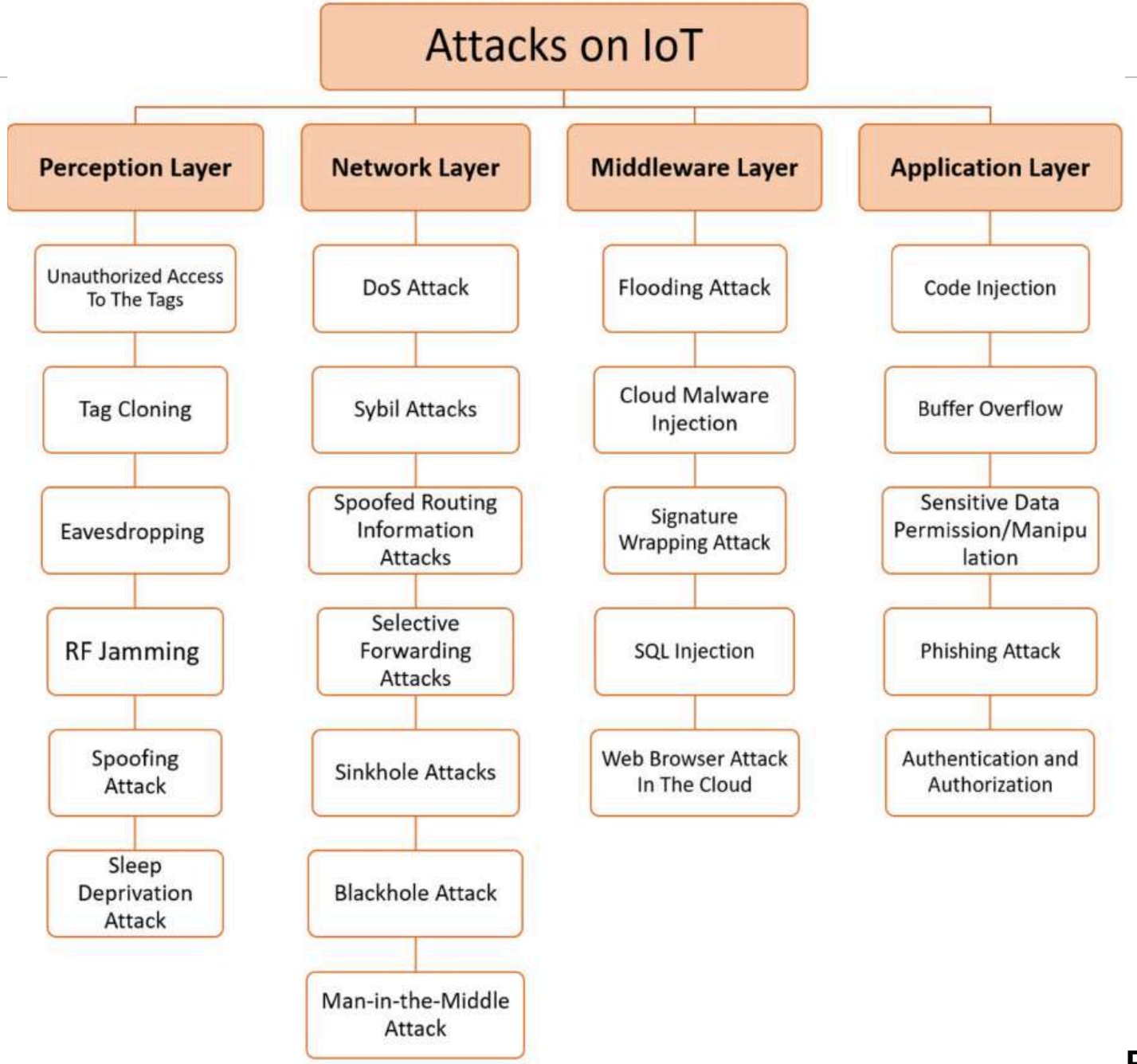


- Supervised Learning
- Unsupervised Learning
- Semi-Supervised Learning
- Reinforcement Learning

Types of IoT attacks

Network Layer

Middleware Layer



IoT Challenges and Key Attacks

IoT Challenges

- Lack of robust authentication and encryption protocols.
- Resource constraints limit strong security measures.
- Privacy concerns due to the collection of sensitive data.

Key Target IoT Attack Types

- Reconnaissance Attacks
- Vulnerability Exploitation: System Vulnerabilities and Unpatched Weaknesses
- Data Exfiltration: Compromised Privacy and Data Security

Literature Review

Machine Learning for IoT Security

Method	Description	Existing work
Anomaly Detection	Uses ML to identify unusual patterns, alerting to potential threats by flagging behaviors outside of normal activity.	Thompson et al.(2020), Kim et al.(2021) Pathak et al.(2021), Bilakanti et al.(2024)
Intrusion Detection	Classifies network traffic as safe or malicious, strengthening defenses against unauthorized access in IoT networks.	Kim et al.(2020), Duhayyim et al.(2023), Sharma et al. (2024), Hizal et al. (2024)
Predictive Analytics and Malware Detection	Predicts future threats and identifies malware, allowing proactive security measures to isolate malicious activity.	Yeboah-Ofori et al. (2021), Alomiri et al. (2024), Duary et al. (2024), Habeeb et al. (2024)

Literature Review

Cyber Deception Techniques in IoT Security

Fake object

- Deploying fake objects to mislead attackers - Zhu et al (2021).
- Studying attack patterns and behaviors in a controlled environment Thompson et al.(2020), Kim et al.(2021).
- Requires careful management to avoid unintended consequences.

Honeypot

- Misleading attackers using deceptive elements like honeypots.
- Gathering intelligence on attacker tactics and delaying their progress.

Literature Review

Type of honeypot

Types of Honeypots	Description	Advantage	Limitation	Existing work
Low-Interaction Honeypots	Simple emulations to gather data on common attack methods	Easy to implement	Easy to be detected by attacker	Honeyd(2002), U-PoT (2021)
High-Interaction Honeypots	Real systems to collect detailed information on advanced attack techniques	Sophisticated and difficult to detect	Deployment and maintenance cost	SIPHON (2010), Honware (2011)
Medium-Interaction Honeypots:	Balance between low and high interaction honeypots	Relatively easy to implement	Static	IoTPOT (2016), Honeycam(2022)

Literature Review

Intelligent-Interaction Honeypots

- This concept involves interacting with attackers to maximize the likelihood of catching the attacks.
- Emulate full devices.
- Use machine learning to learn from attacker behavior and improve deception techniques.

- IoTCandyJar by Luo et al.(2018): IoTCandyJar honeypots take some time until they can respond appropriately to requests.
- FirmPot byMoeka et al.(2021): The honeypots generated by this framework do not capture any advanced attack such as configuration changes.

Gaps in Existing Work and Contributions of This Thesis

Identified Gaps:

- Static Deception Strategies: Lack real-time adaptability.
- Limited Integration: Rare combination of machine learning with dynamic deception strategies.
- Scalability Issues: High-interaction honeypots require significant resources.

Our Thesis

By leveraging Reinforcement Learning combined with machine learning models, we can create a proactive security system that adapts to the expansion of the number of IoT devices.

Key Contributions

C1

Adaptive intelligent interaction honeypot system

Engages and misleads attackers, capturing valuable data on their methods.

C2

Hybrid recommender system leveraging adaptive learning

Combines real and deceptive data to confuse attackers and reduce successful breaches.

C3

Augmented reality-based honeypot for IoT cameras

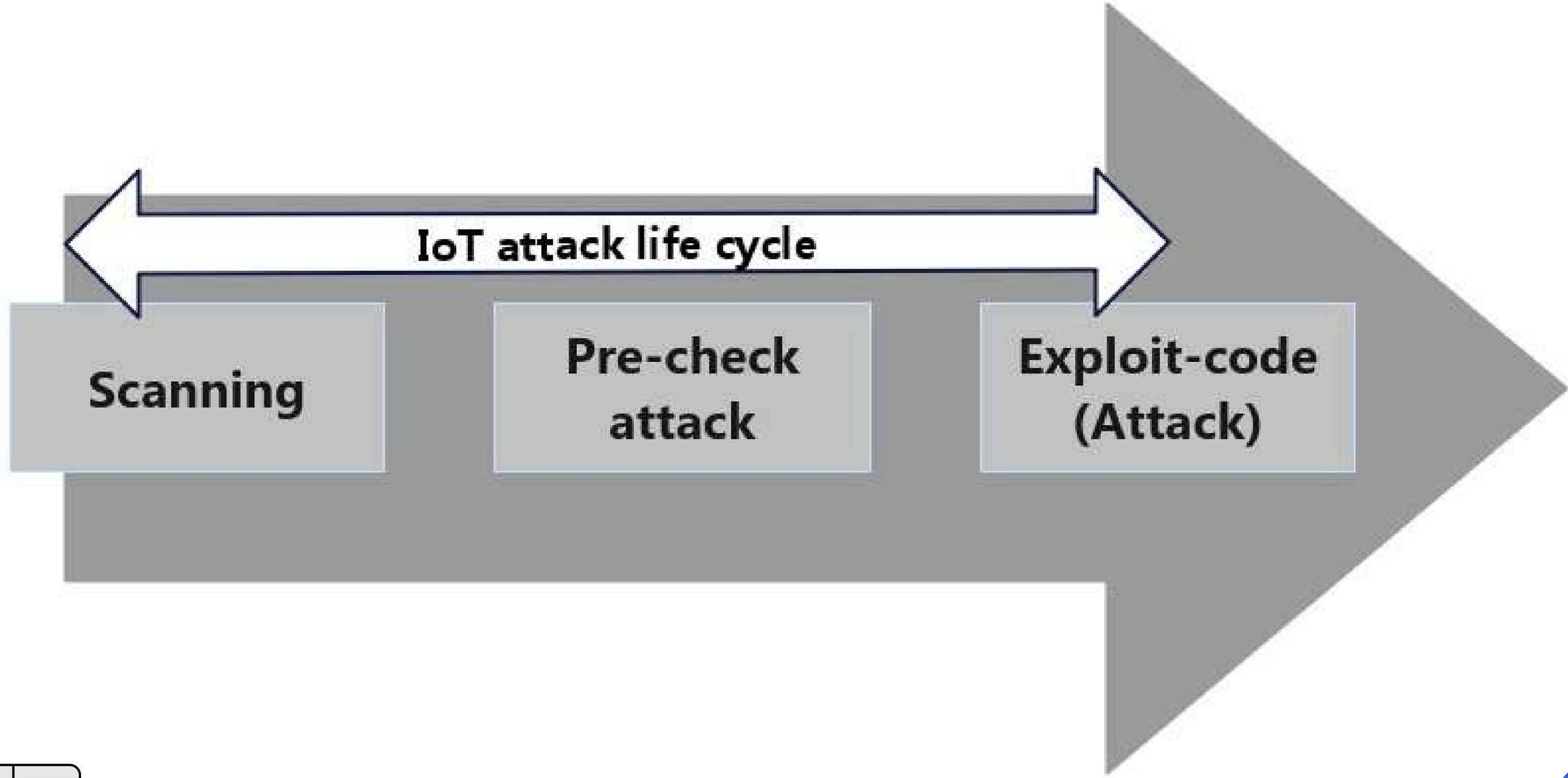
Creates realistic, interactive decoys for IoT cameras, gathering detailed intelligence on attacker strategies.

Contribution 1

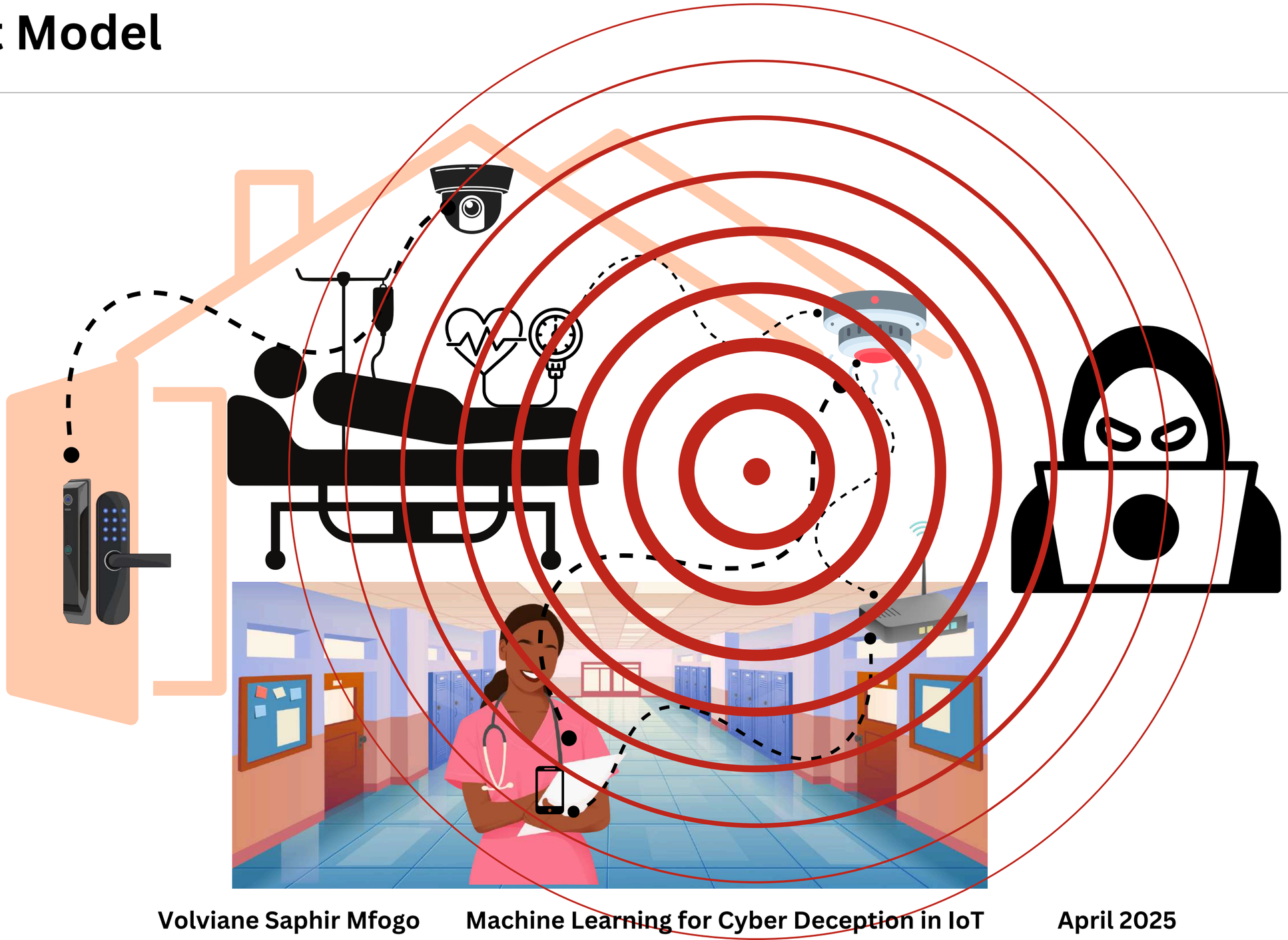
Adaptive Intelligent Cyber Deception for Probing Attacks on IoT Devices

V.S Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack and C. Kamhoua, "AIIPot: Adaptive Intelligent-Interaction Honeypot for IoT Devices," 2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Toronto, ON, Canada, 2023

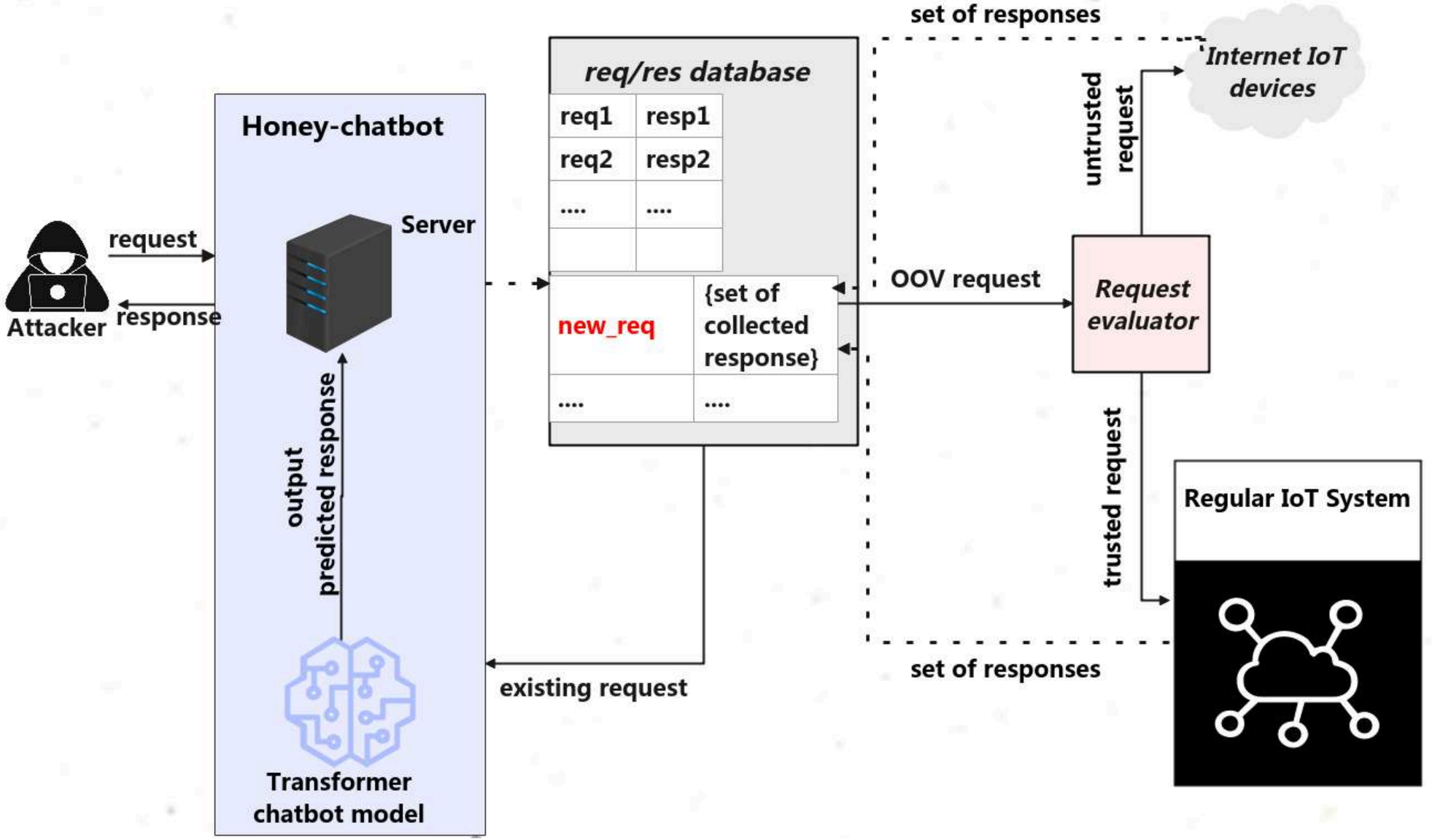
Motivation


IoT attack life cycle
Scanning
Pre-check attack
Exploit-code (Attack)

Threat Model



System Overview



V.S Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack and C. Kamhoua, . Aiipot: Adaptive intelligent-interaction honeypot for IoT devices. In 2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, Toronto, ON, Canada, 2023, pp. 1-6, doi:10.1109/PIMRC56721.2023.10293827

Req/Res Database

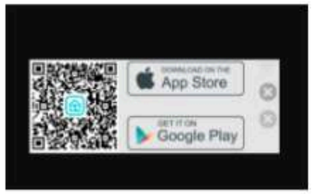
http://34.64.188.58/favicon.ico

Request

method	path	query	header	body	response id
GET	/favicon.ico	<EMP>	Accept.	<EMP>	1

Response

response id	status	header	boby
1	200	'application/ octet-stream'	..... \x00\x00\x01\x0 0\x05\x00€€....

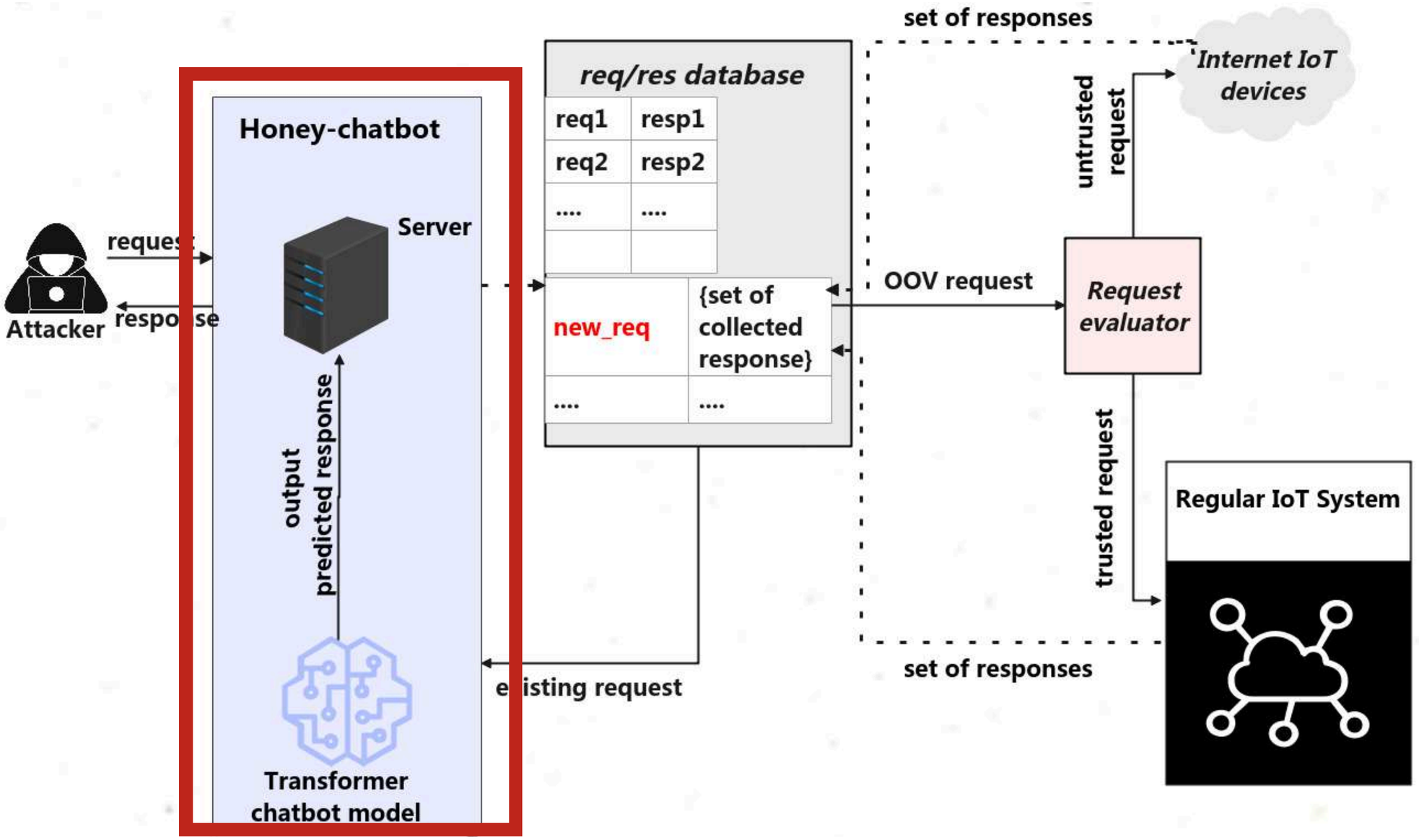


request 1

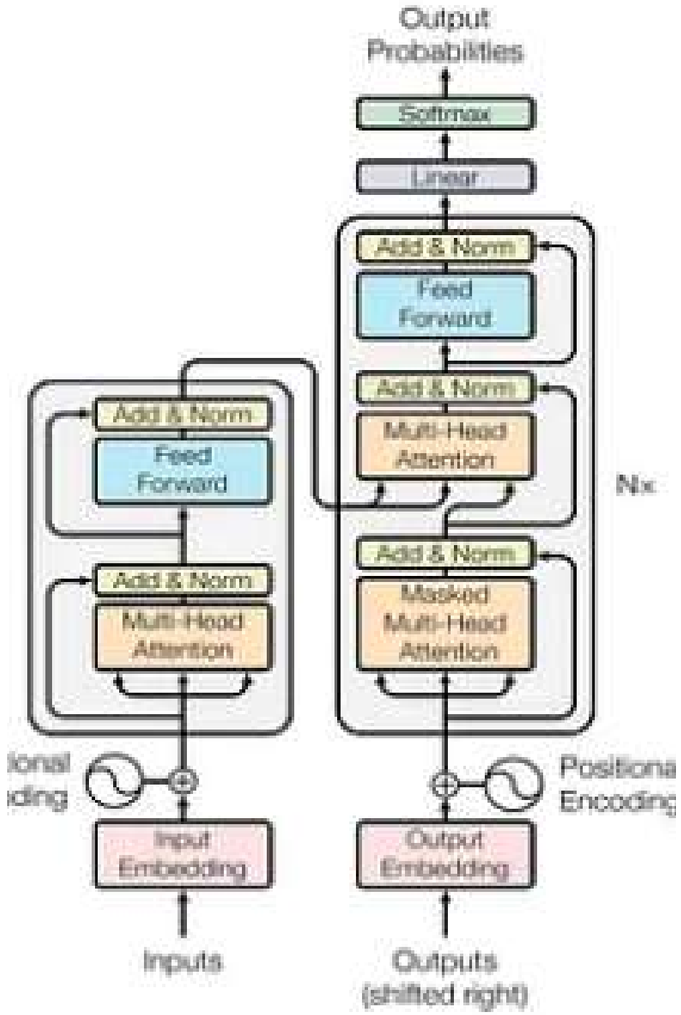
- response device 1
- response device 2
- ....
- response device n

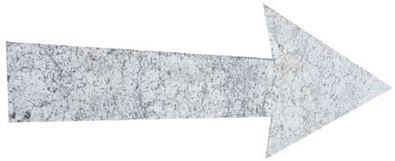
request 1	response device 1
request 1	response device 2
...	....
request 1	response device n

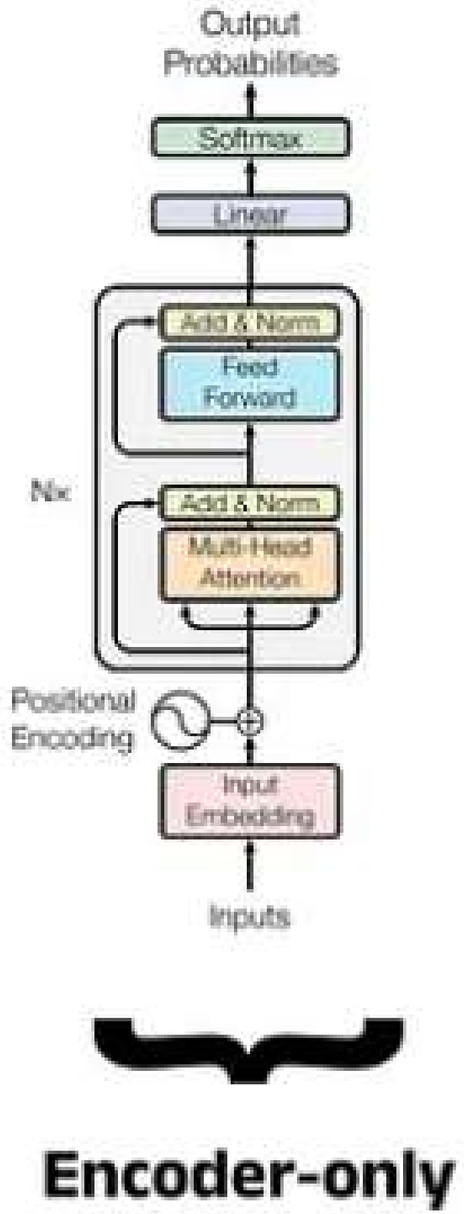
Intelligent Interaction Honeypot: Honey-Chatbot



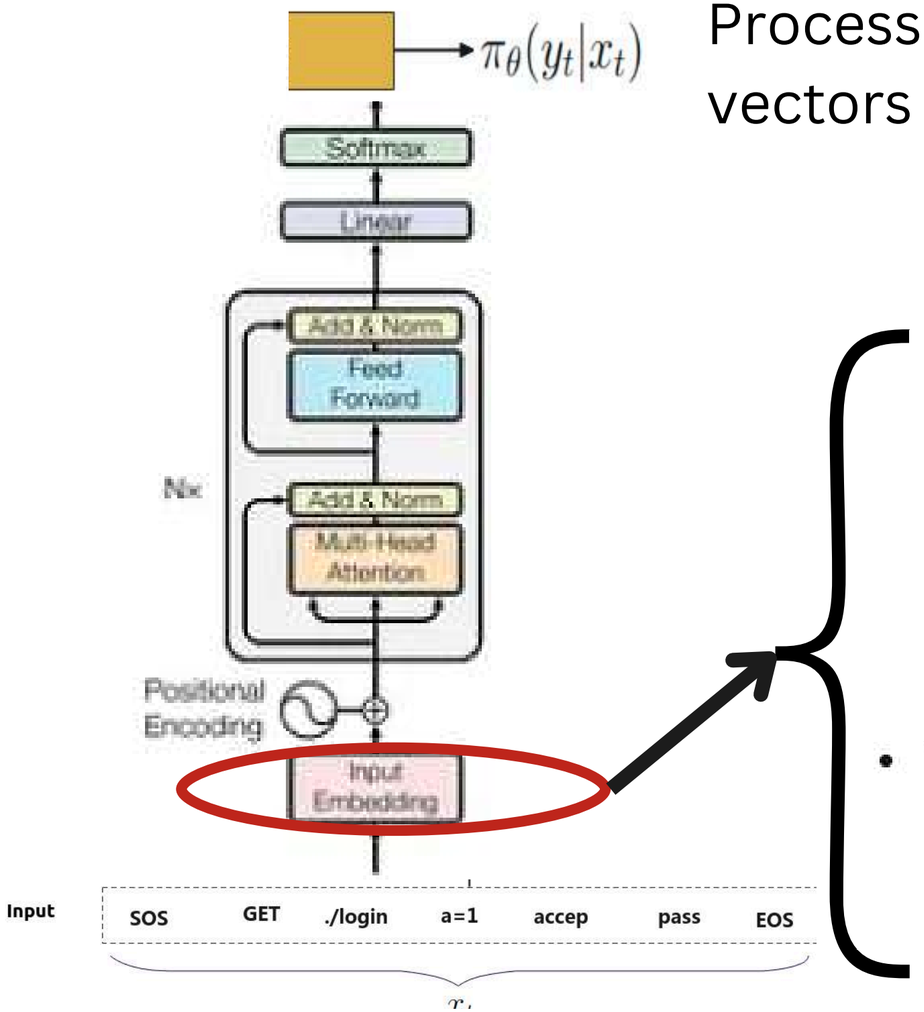
Bidirectional Encoder Representations from Transformers(BERT)







Bidirectional Encoder Representations from Transformers(BERT)



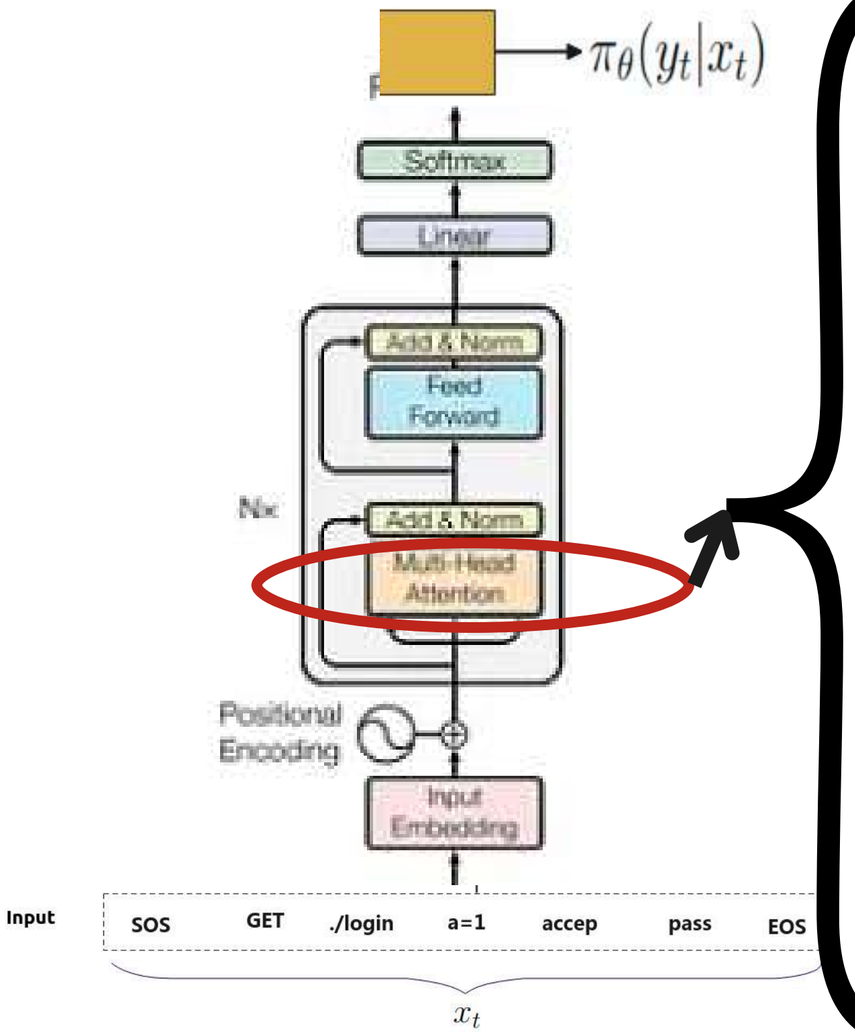
Process of converting input data (e.g., words or tokens) into dense vectors of fixed size, which can be processed by the BERT model.

- **Token Embedding:** $\mathbf{E}_{\text{token}}$
- **Segment Embedding:** $\mathbf{E}_{\text{segment}}$
- **Position Embedding:** $\mathbf{E}_{\text{position}}$

- For each token t_i in the input sequence, the final input embedding $\mathbf{E}_i$ is computed as:

$$\mathbf{E}_i = \mathbf{E}_{\text{token}}(t_i) + \mathbf{E}_{\text{segment}}(s_i) + \mathbf{E}_{\text{position}}(p_i)$$

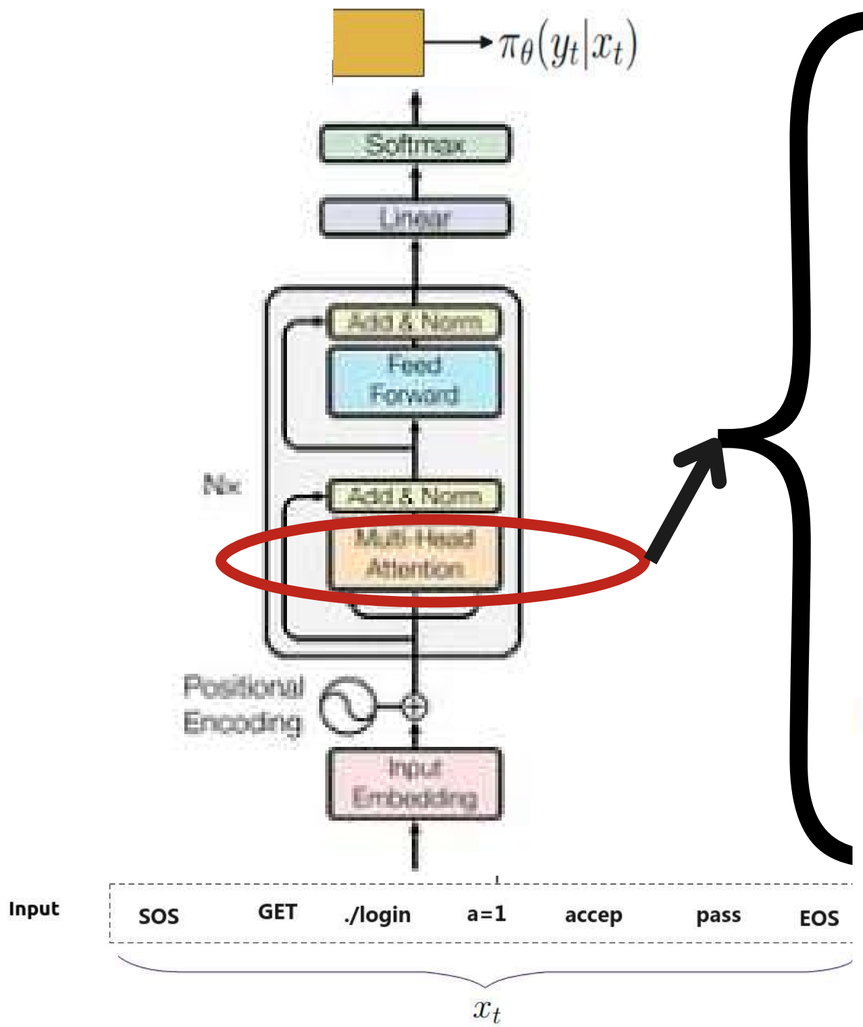
Bidirectional Encoder Representations from Transformers(BERT)



Multi-head attention allows BERT to focus on different parts of the input sequence simultaneously, capturing various relationships and dependencies between tokens.

- Query Q: Represents the current token for which attention is being calculated.
- Key K: Represents the tokens being compared against the query.
- Value V: Represents the information retrieved from the tokens based on the attention score.

Bidirectional Encoder Representations from Transformers(BERT)



$$\text{Attention}(\mathbf{Q}, \mathbf{K}, \mathbf{V}) = \text{softmax}\left(\frac{\mathbf{Q}\mathbf{K}^\top}{\sqrt{d_k}}\right)\mathbf{V}$$

where:

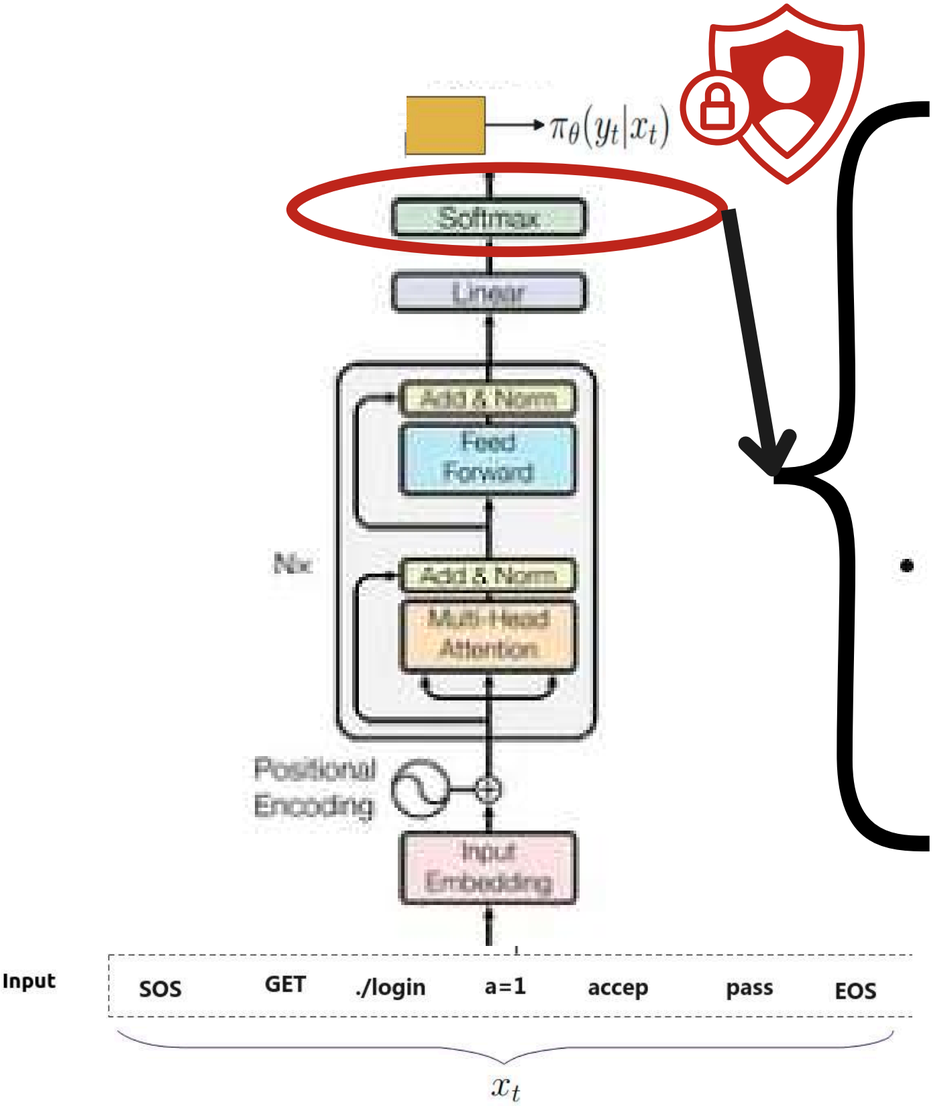
- $\mathbf{Q} = \mathbf{X}\mathbf{W}_\mathbf{Q}$
- $\mathbf{K} = \mathbf{X}\mathbf{W}_\mathbf{K}$
- $\mathbf{V} = \mathbf{X}\mathbf{W}_\mathbf{V}$
- $\mathbf{X}$ is the input sequence, and $\mathbf{W}_\mathbf{Q}, \mathbf{W}_\mathbf{K}, \mathbf{W}_\mathbf{V}$ are learned weight matrices.
- d_k is the dimension of the key vectors (used for scaling).

Multi-Head Attention:

- Multi-head attention combines the outputs from multiple attention heads:

$$\text{MultiHead}(\mathbf{Q}, \mathbf{K}, \mathbf{V}) = \text{Concat}(\text{head}_1, \text{head}_2, \ldots, \text{head}_h)\mathbf{W}_\mathbf{O}$$

Bidirectional Encoder Representations from Transformers(BERT)

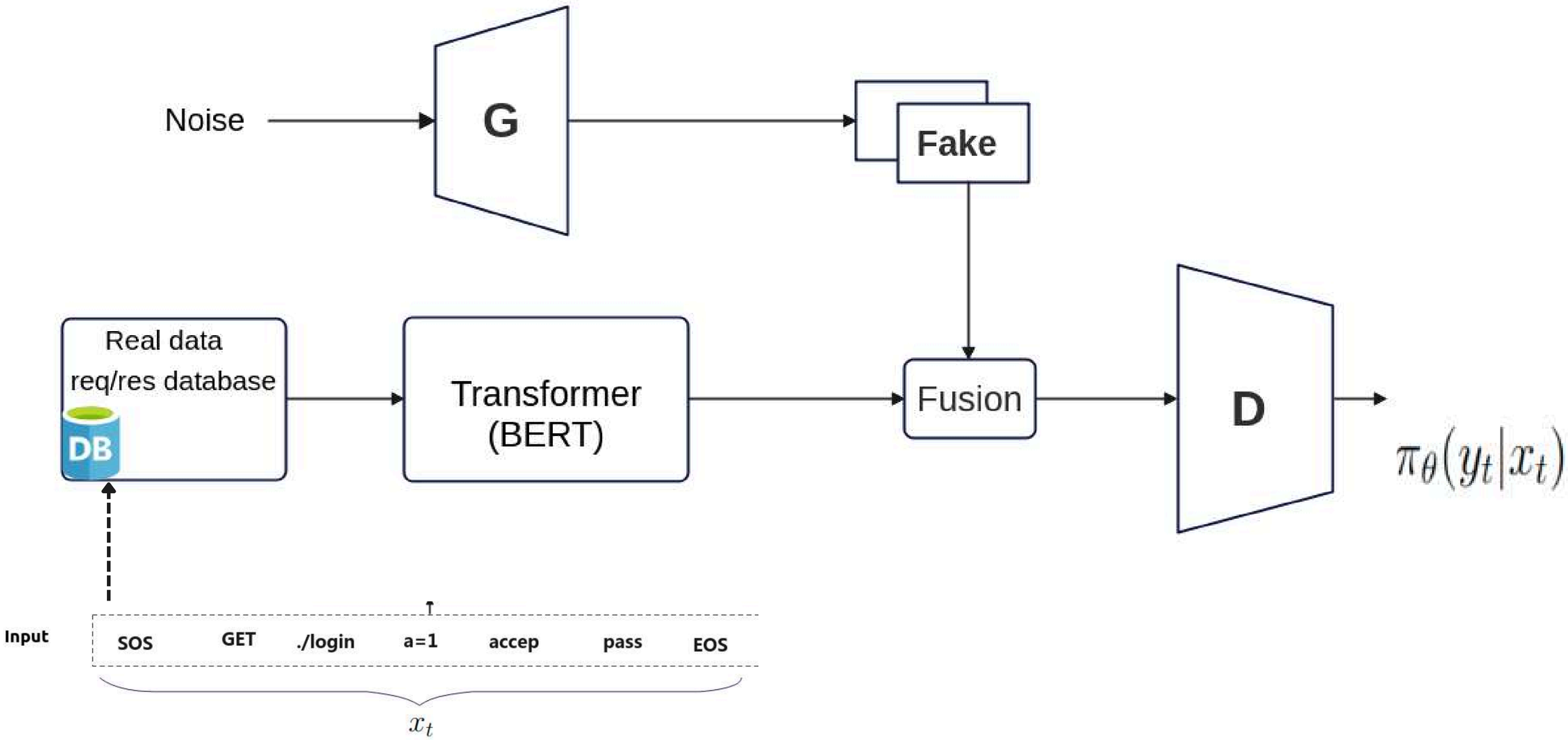


- Converts a vector of raw scores (logits) into probabilities. It is widely used in BERT for normalizing attention scores and for the final classification layer.

- Given a vector of logits $z = [z_1, z_2, \ldots, z_n]$, the softmax function is defined as:

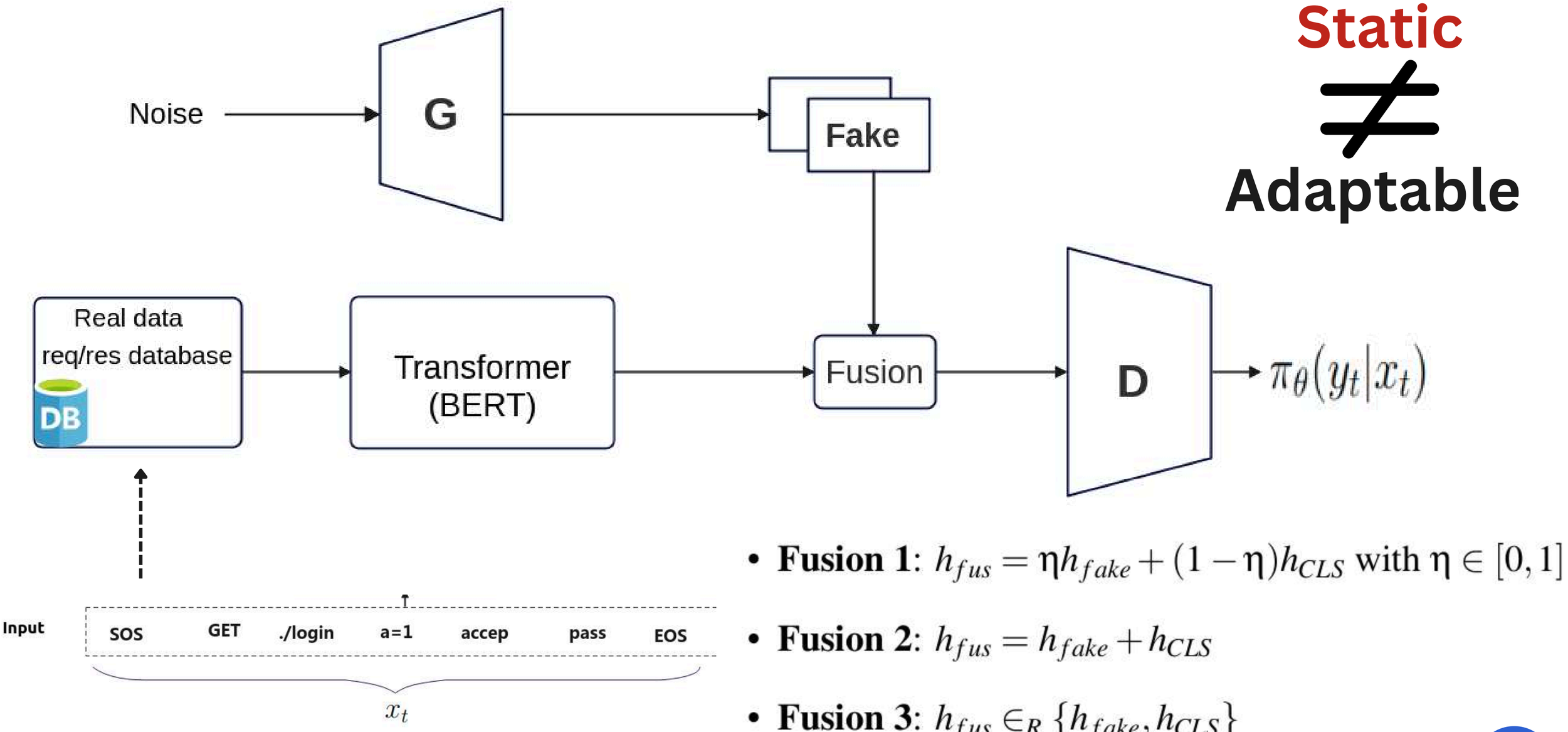
$$\text{Softmax}(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_j}}$$

GAN & BERT



V.S Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack and C. Kamhoua, "GAN-AIIPot: GAN-based Cyber Deception for Probing Attacks on IoT Devices," IEEE Transactions on Network and Service Management.

GAN & BERT



Static

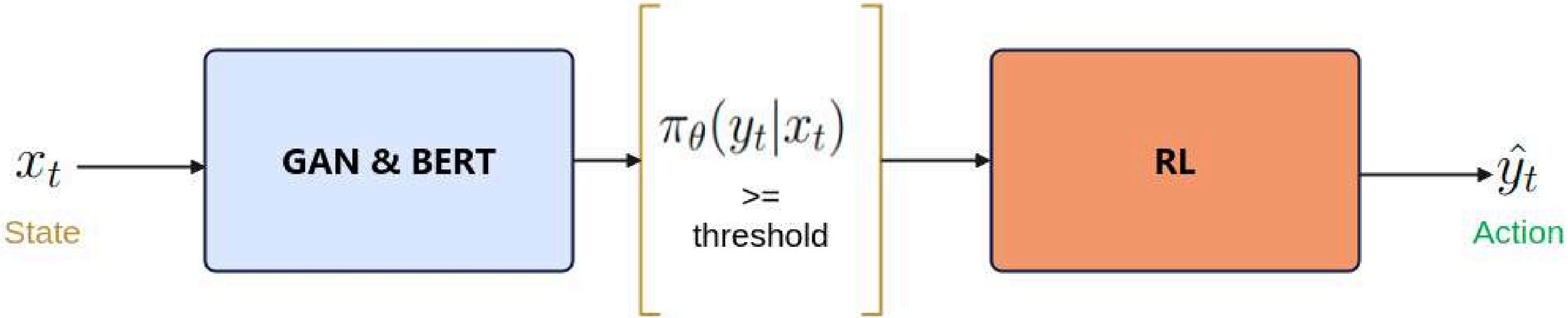
$\neq$

Adaptable

- **Fusion 1**: $h_{fus} = \eta h_{fake} + (1-\eta) h_{CLS}$ with $\eta \in [0,1]$
- **Fusion 2**: $h_{fus} = h_{fake} + h_{CLS}$
- **Fusion 3**: $h_{fus} \in_R \{h_{fake}, h_{CLS}\}$

Adaptive Intelligent Interaction Honeypot

- **Threshold Decision ($\pi_\theta(y_t|x_t)$):** The output of GAN & BERT is compared against a predefined threshold to determine the optimal action probability.
- **Reinforcement Learning (RL):** The RL model then uses this probability to decide the best action $\hat{y}_t$ to take, adapting in real-time to evolving threats.



- **State** = Request
- **Action**= Response
- **Reward**= +1 if a new request is sent and -1 if not

Learning process

Action Selection: Balancing Exploration and Exploitation

The **ε-greedy policy** is a strategy used in RL to ensure that the model doesn't just exploit known actions but also explores new ones to potentially discover better strategies.

Given the current state x_t, the action y_t is chosen according to the ε-greedy policy:

$$y_t = \begin{cases} \text{random action}, & \text{with probability } \varepsilon \\ \arg\max_y Q(x_t, y), & \text{with probability } 1 - \varepsilon \end{cases}$$

Adaptability: This approach ensures that the system remains flexible and capable of adapting to new, unforeseen threats by not always following a fixed strategy.

Performance Evaluation

Dataset and GAN & BERT model training setup

- Dataset: Emulated Website (HTTP protocol) provided by Firmpot ~ 100 000 entries
- Epoch: 75 000 epoch
- The initial learning rate is set to 0.001 and the batch size is 512.
- Deployment on the Google Cloud platform in 20 days
- Comparison: (IoTCandyjar, 2018), (Firmpot, 2021)

Training Result

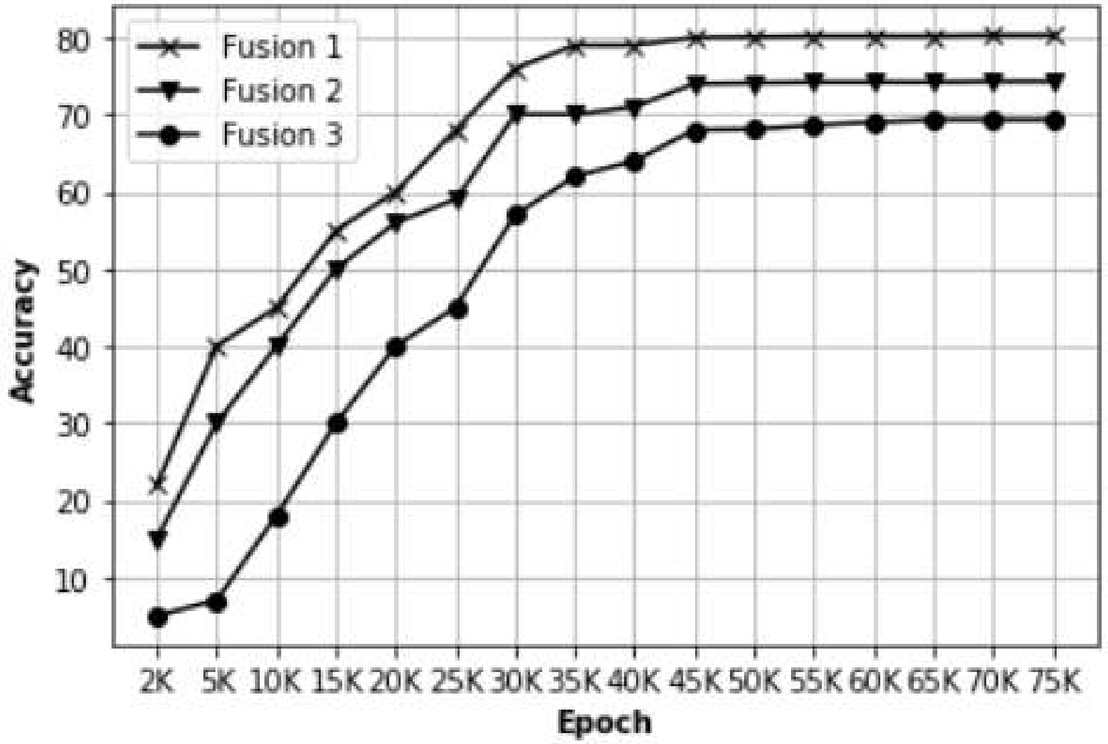


Figure 1 – Learning curve of the model with different fusion methods.

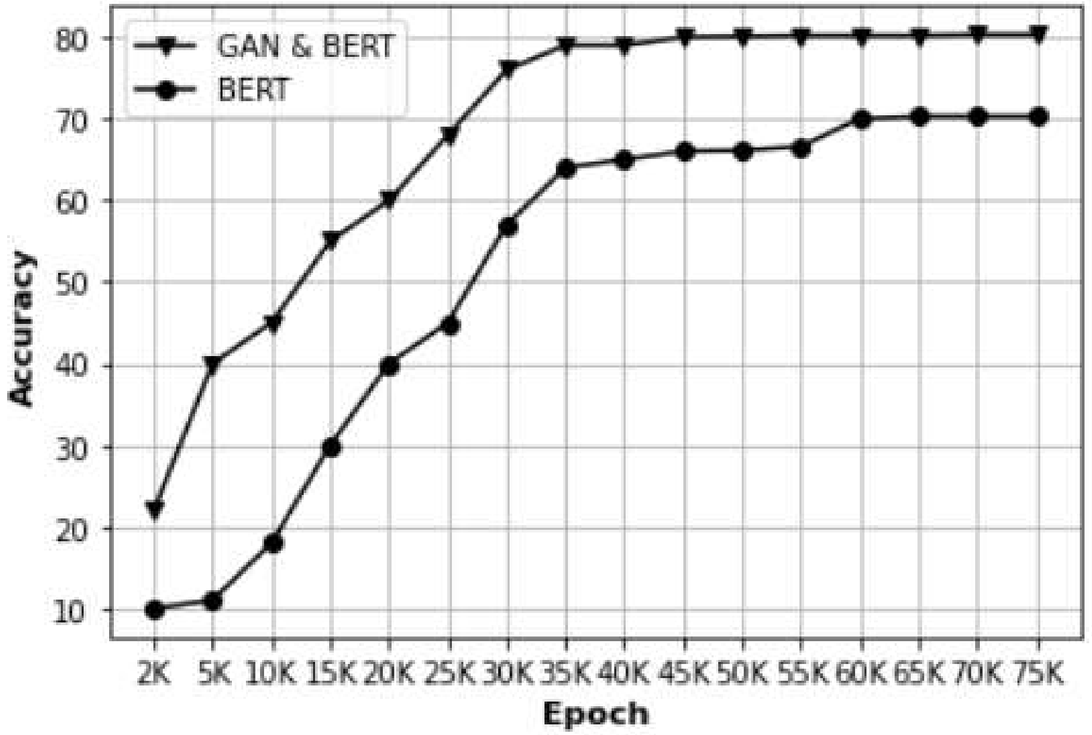
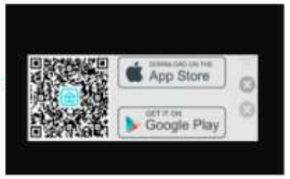
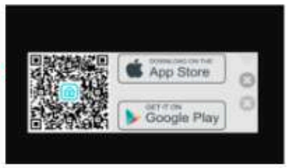


Figure 2 – Learning curve of the proposed GAN & BERT model with the best fusion method.

Evaluation & Result

GAN & BERT output

Request	http://34.64.188.58/favicon.ico	http://34.64.188.58/webpages/locale/language.js	https://34.64.188.58/cgi-bin/luci/;stok=/login
Possible status code response	status code: 200 	**Not Found** Status code: 404	**Internal Server Error** Status code: 500
Model output	status code: 200 	**Unauthorized** Status code: 401	**Internal Server Error** Status code: 500

Method	Total number of requests received / total number of IP addresses observed
GAN-AIIPot	9,235/1287
AIIPot	6,235/987
Firmpot	2,896/687

Evaluation & Result

Deception Effectiveness : Session length

Figure 3 – Session length comparison between attackers and honeypots (in percentage).

Evaluation & Result

Deception Effectiveness : Data captured and attack detected

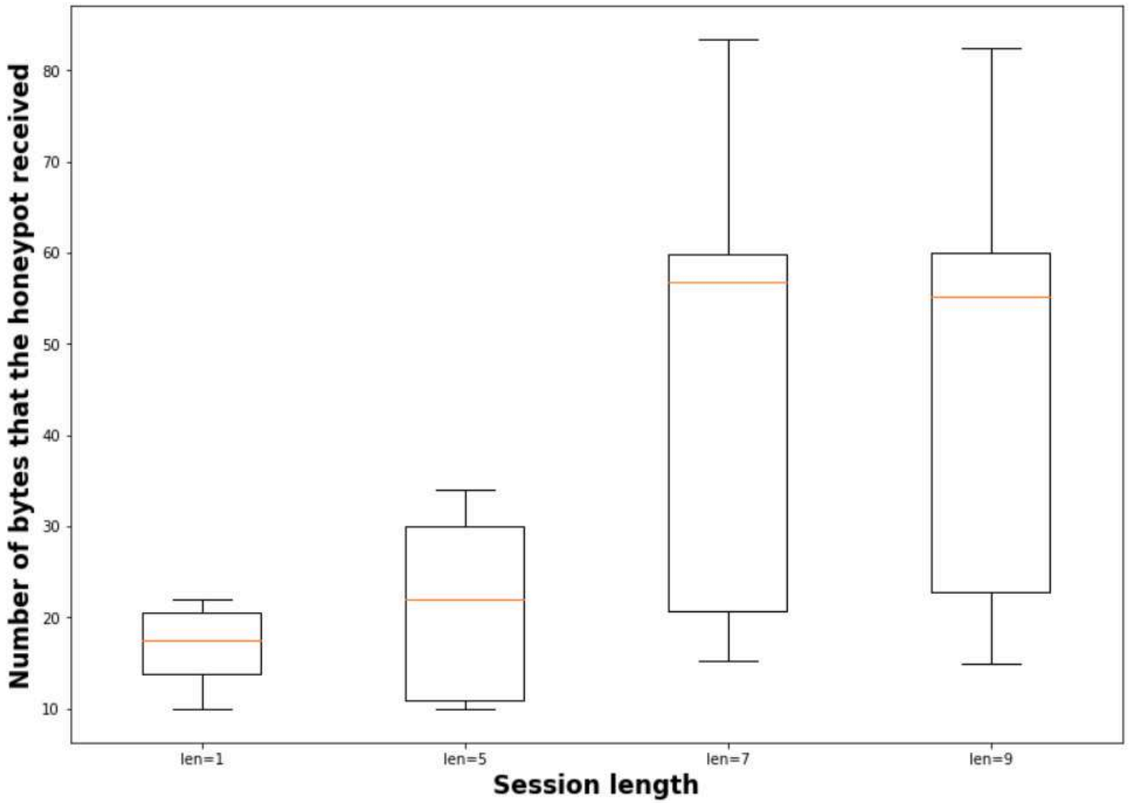


Figure 4 – The amount of information received by the proposed honeypot per session length.

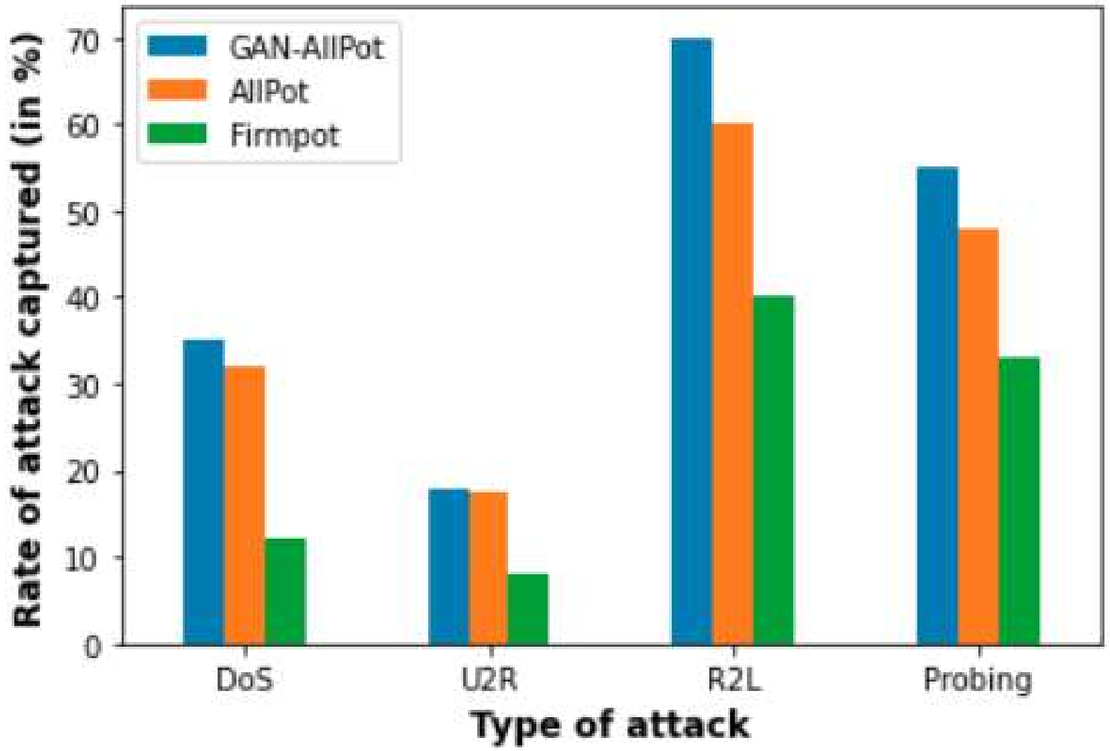


Figure 5 – The count of attacks detected by the honeypot categorized according to the NSL-KDD dataset.

Analysis & DISCUSSION

Effectiveness of GAN-AIIPot:

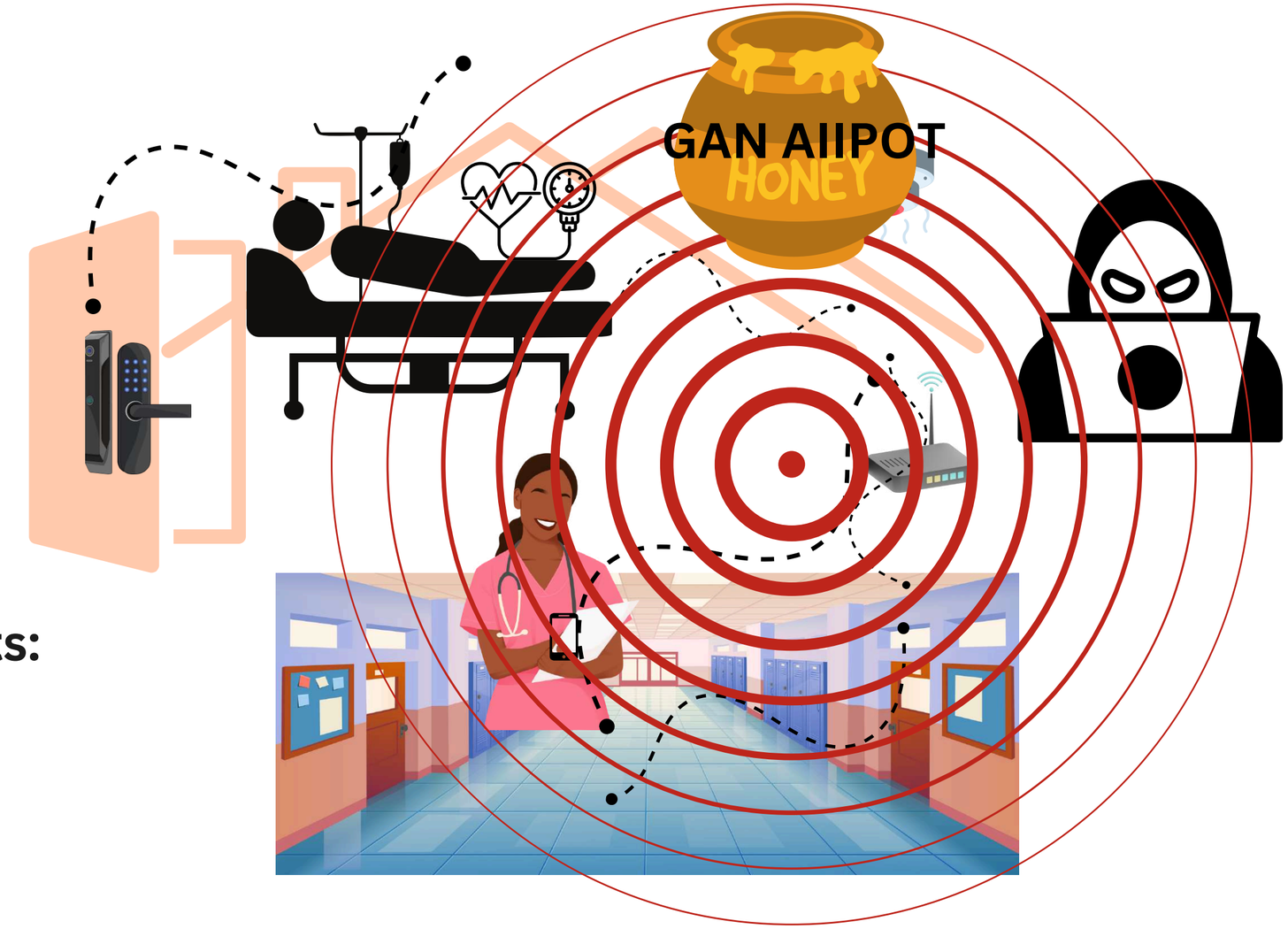
- Vulnerability Detection
- Enhanced Detection

Adaptive Cyber Deception:

- Extended Engagement
- Dynamic Learning

Advantages Over Traditional Honeypots:

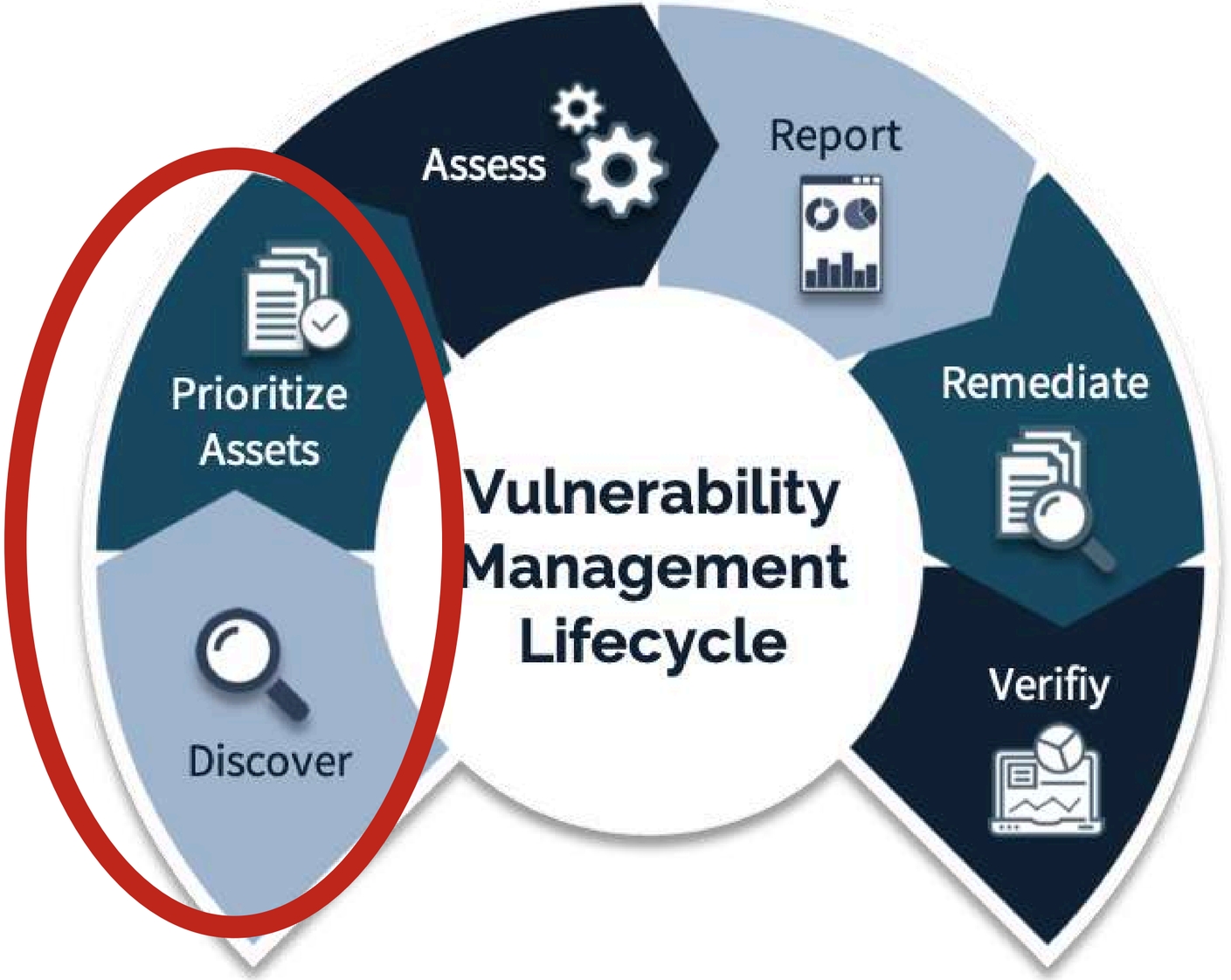
- Adaptive & Scalable
- Continuous Improvement



Contribution 2

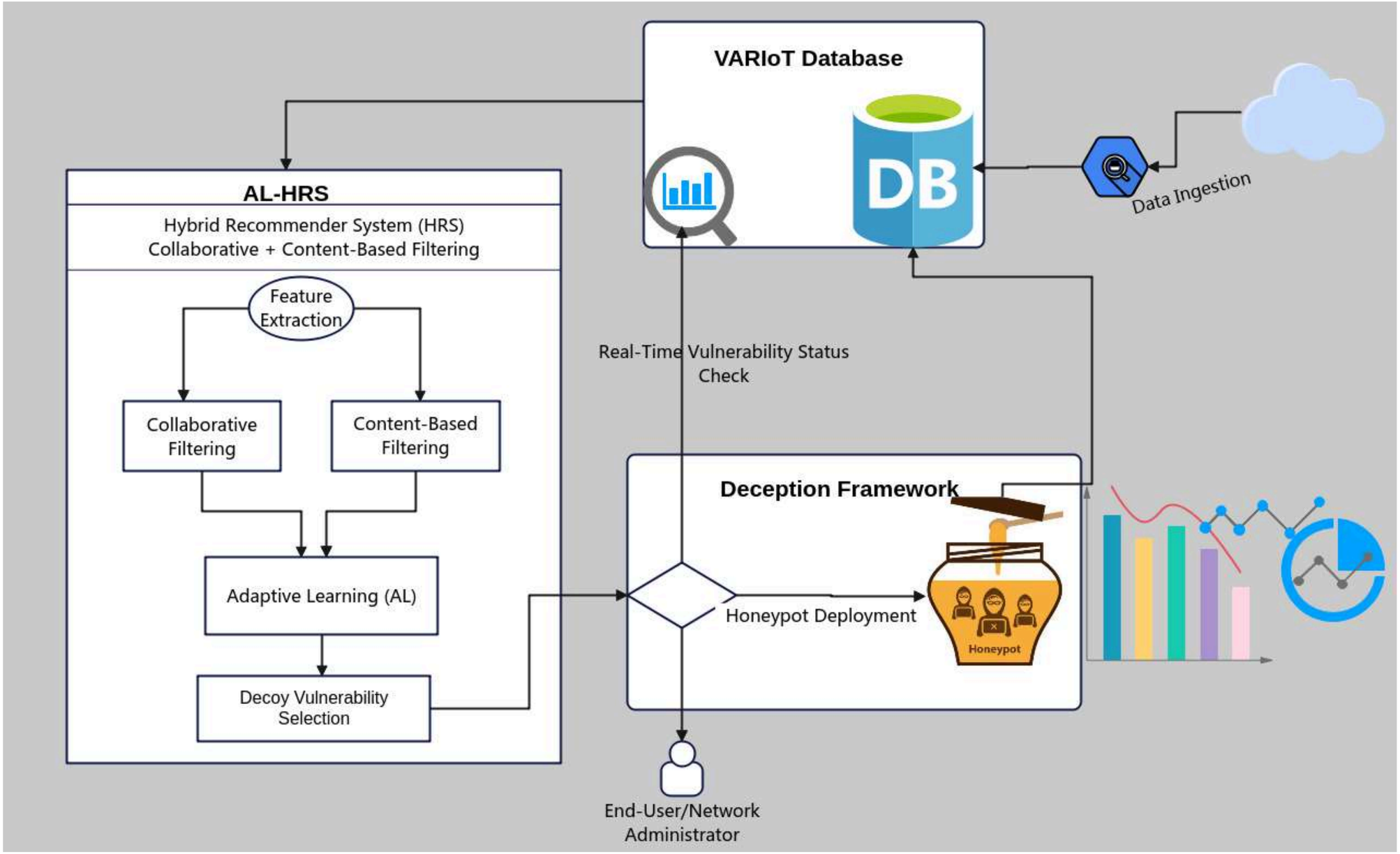
Adaptive Learning for IoT Security: A Hybrid Recommender System Approach

Motivation

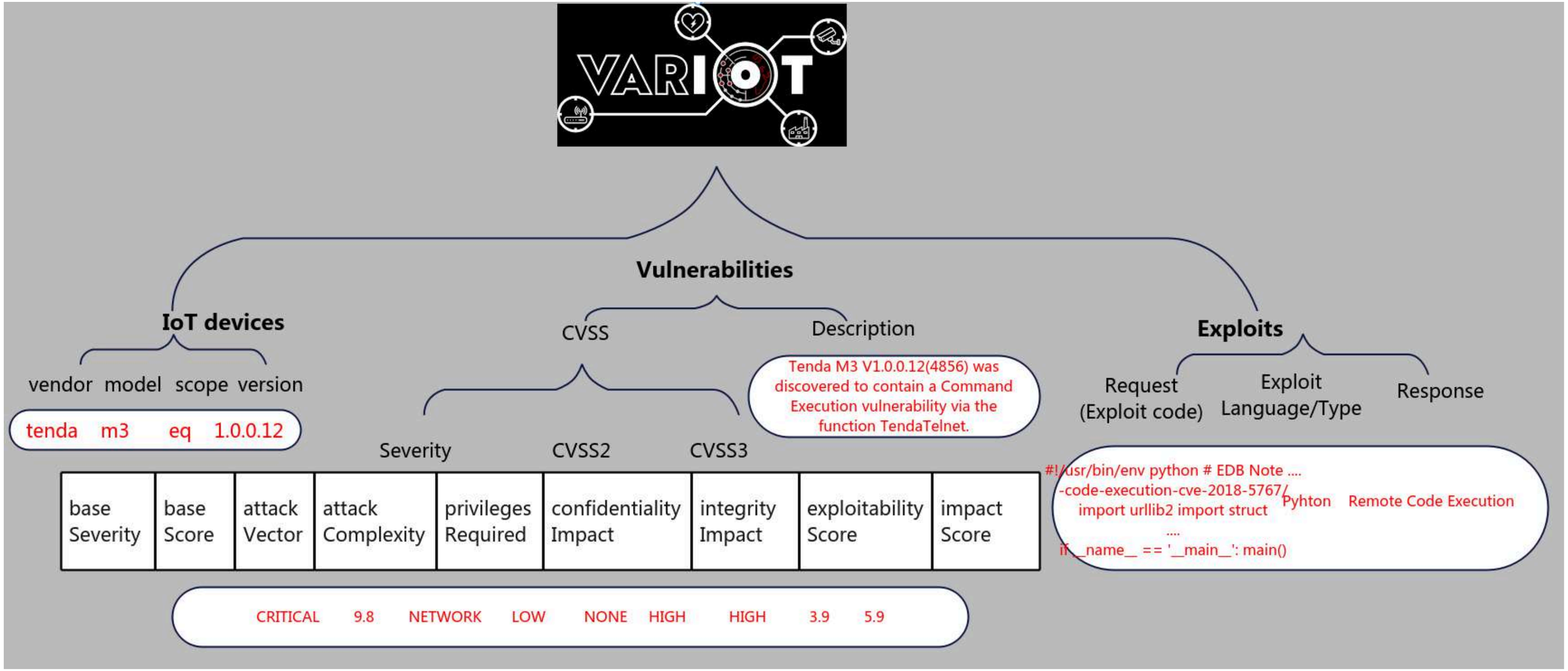

Assess
Report
Prioritize Assets
Remediate
Vulnerability Management Lifecycle
Verifiy
Discover

Threat Model

System Overview



VARIoT Database



Hybrid recommender System 1/4

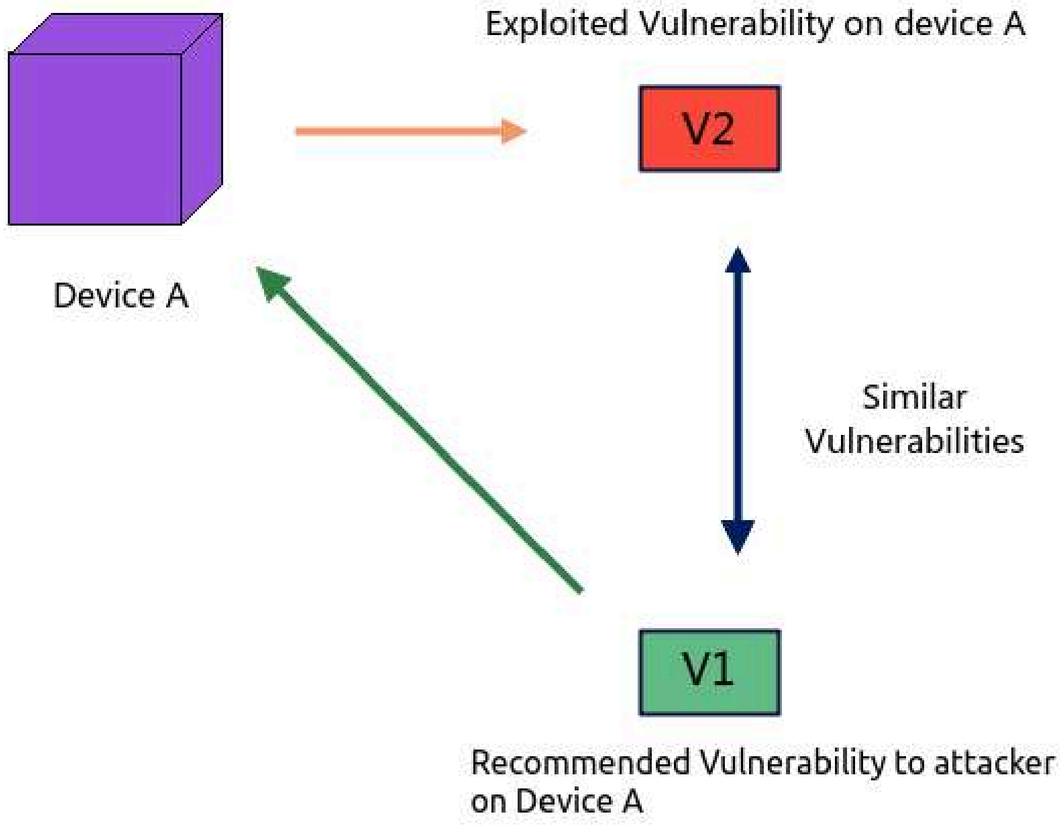


Figure 6: Content-based filtering

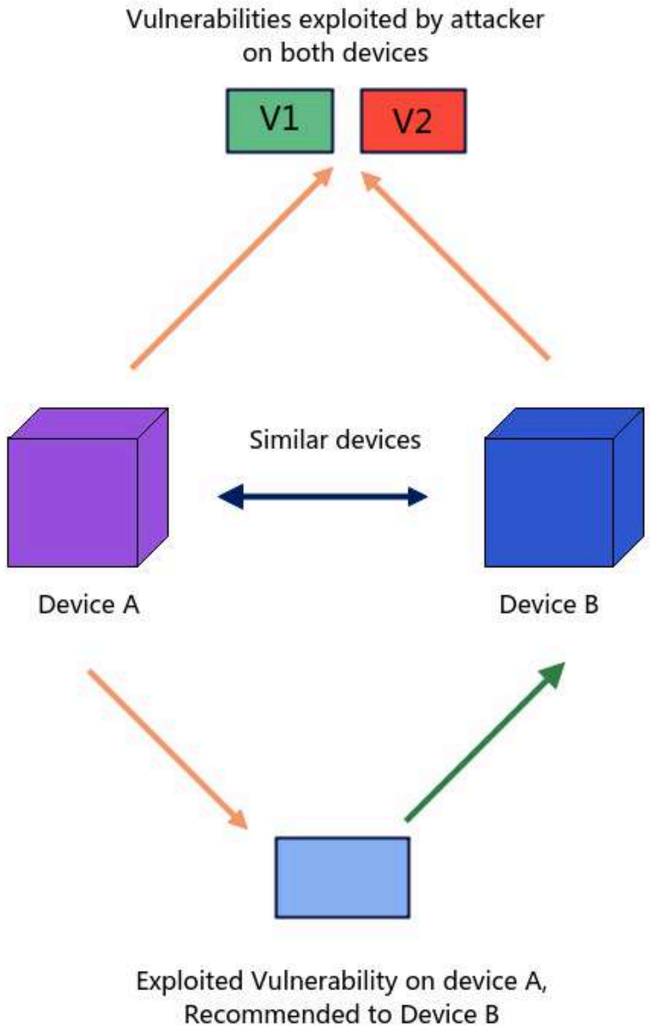


Figure 7: Collaborative filtering for recommended vulnerability

Hybrid recommender System 2/4

$$\text{Score}(v_j, d_i) = \theta_{CF} \cdot \text{CF_Score}(v_j, d_i) + \theta_{CBF} \cdot \text{CBF_Score}(v_j, d_i),$$

where:

- θ_{CF} and θ_{CBF} are the adaptive weights assigned to the outputs from CF and CBF, respectively;
- $\text{CF_Score}(v_j, d_i)$ quantifies the relevance of a vulnerability based on interaction patterns of attackers with similar profiles;
- $\text{CBF_Score}(v_j, d_i)$ reflects the relevance based on the intrinsic attributes of the vulnerabilities and device profiles.

Hybrid recommender System 3/4

$$\text{CF_Score}(v_j, d_i) = \frac{\sum_{k \in \mathcal{N}(d_i)} \text{sim}(d_i, d_k) \cdot r_{k,j}}{\sum_{k \in \mathcal{N}(d_i)} \text{sim}(d_i, d_k)} \quad \text{with} \quad \text{sim}(d_i, d_k) = \frac{\mathbf{f}_d(d_i) \cdot \mathbf{f}_d(d_k)}{\|\mathbf{f}_d(d_i)\| \cdot \|\mathbf{f}_d(d_k)\|}$$

$$\Rightarrow \quad \text{CF_Score}(v_j, d_i) = \frac{\sum_{k \in \mathcal{N}(d_i)} \frac{\mathbf{f}_d(d_i) \cdot \mathbf{f}_d(d_k)}{\|\mathbf{f}_d(d_i)\| \cdot \|\mathbf{f}_d(d_k)\|} \cdot r_{k,j}}{\sum_{k \in \mathcal{N}(d_i)} \frac{\mathbf{f}_d(d_i) \cdot \mathbf{f}_d(d_k)}{\|\mathbf{f}_d(d_i)\| \cdot \|\mathbf{f}_d(d_k)\|}}$$

- $\mathbf{f}_d(d_i)$ and $\mathbf{f}_d(d_k)$ are the feature vectors of devices d_i and d_k, respectively.
- $\|\mathbf{f}_d(d_i)\|$ denotes the Euclidean norm (or length) of the feature vector $\mathbf{f}_d(d_i)$.
- The dot product $\mathbf{f}_d(d_i) \cdot \mathbf{f}_d(d_k)$ measures the degree of alignment between the two feature vectors, indicating how similar the two devices are.

Hybrid recommender System 4/4

$$\text{CBF_Score}(v_j, d_i) = \mathbf{w}_v \cdot \mathbf{f}_d$$

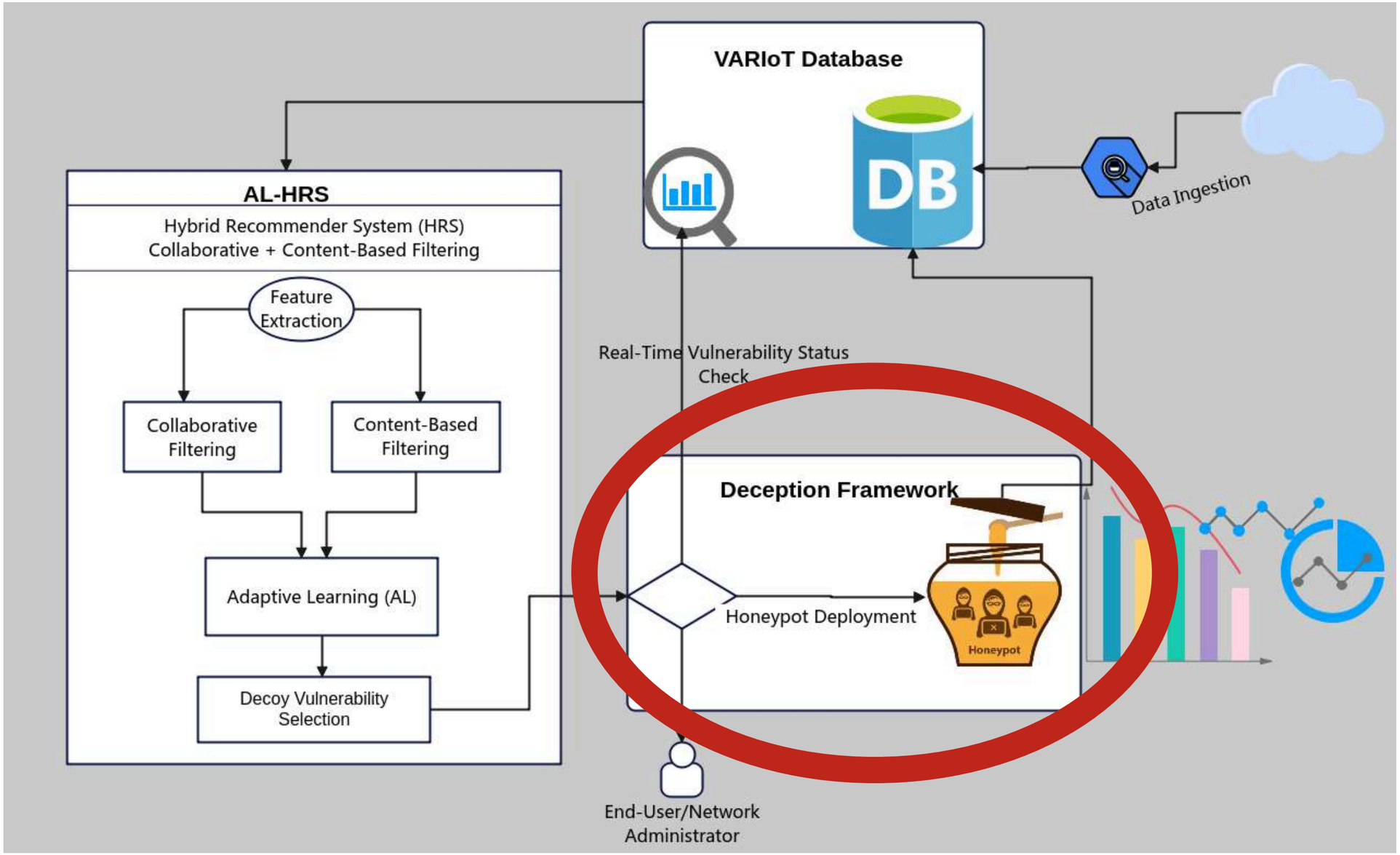
$$\mathbf{w}_v = [w_{v1}, w_{v2}, \ldots, w_{vn}] \qquad \mathbf{f}_d = [f_{d1}, f_{d2}, \ldots, f_{dm}]$$

$$\text{Score}(v_j, d_i) = \theta_{CF} \cdot \left(\frac{\sum_{k \in \mathcal{N}(d_i)} \frac{\mathbf{f}_d(d_i) \cdot \mathbf{f}_d(d_k)}{\|\mathbf{f}_d(d_i)\| \cdot \|\mathbf{f}_d(d_k)\|} \cdot r_{k,j}}{\sum_{k \in \mathcal{N}(d_i)} \frac{\mathbf{f}_d(d_i) \cdot \mathbf{f}_d(d_k)}{\|\mathbf{f}_d(d_i)\| \cdot \|\mathbf{f}_d(d_k)\|}} \right) + \theta_{CBF} \cdot (\mathbf{w}_v \cdot \mathbf{f}_d)$$

Adaptive learning for weight optimization

- Markov Decision Process (MDP): A framework used to model decision-making in environments with uncertainty, defined by states, actions, rewards, and transition probabilities.
- States (s): Current security status, including detected attack patterns and known vulnerabilities.
- Actions (a): Choosing vulnerabilities as decoys to mislead attackers.
- Rewards (r): Based on the success of deception, measured by how well attackers are misdirected.
- Transition Probabilities (T): Likelihood of moving between states after an action, influenced by the attacker's response.

Deception Framework



Performance Evaluation

- Dataset: VARIoT, NVD, CVE
- Metric: precision, recall, F1-score, engagement time
- Comparison: Firmpot (2021), AIIPot (2023)

Result

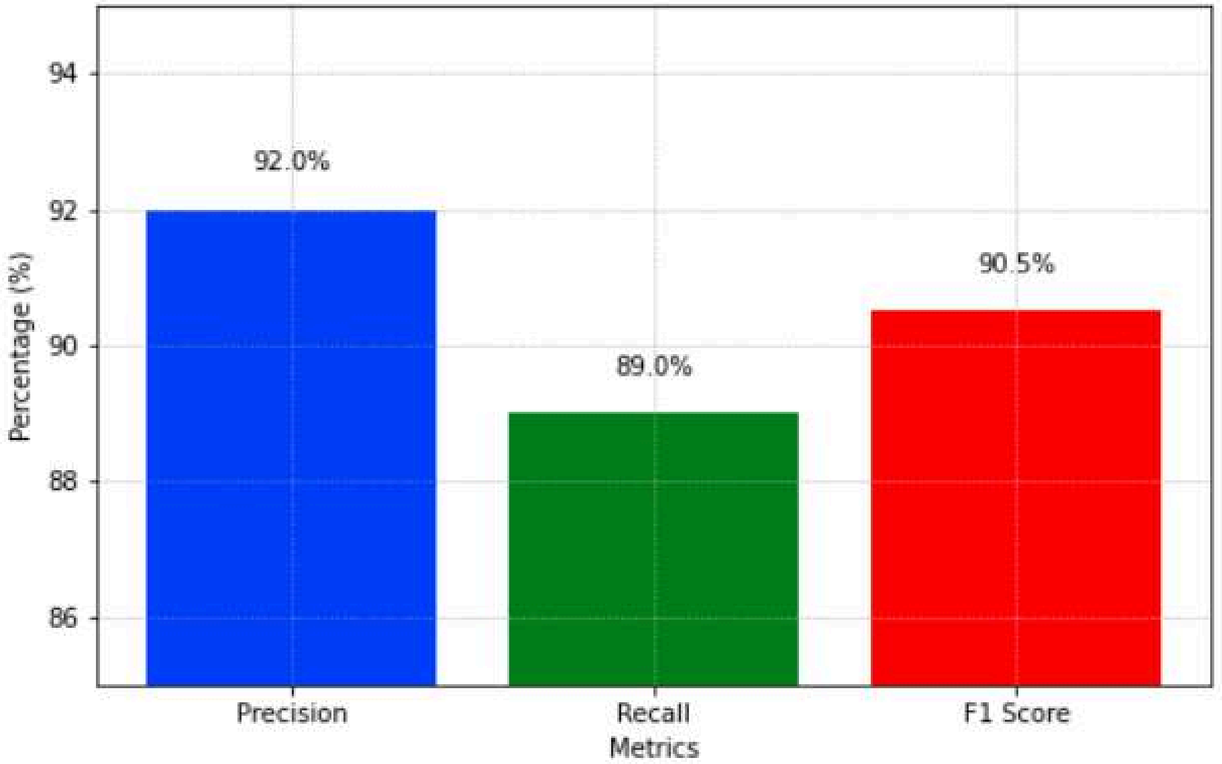


Figure 8 – Average Precision, Recall, and F1 Score of AL-HRS across different testing environments

Table 2 – *Comparison of accuracy metrics across different systems*

System	Precision	Recall	F1 Score
AL-HRS	92%	89%	90.5%
Hybrid CF+CBF	85%	82%	83.5%
CF Only	80%	78%	79.0%
CBF Only	78%	75%	76.5%

Result

Table 3 – *Recommended vulnerabilities for smart home devices.*

Device Type	CVE ID	Recommended vulnerability	CVSS Exploitability	Effectiveness
Smart Thermostat	CVE-2023-5002	Buffer Overflow in Communication Protocol	8.5	High
Smart Light	CVE-2023-5003	Firmware reversion attack	7.1	Medium
Smart Fridge	CVE-2023-5004	Cross-Site Scripting in Web Interface	6.9	Medium
Home Security Camera	CVE-2023-5005	Remote code execution via API	9.8	High
Smart TV	CVE-2023-5006	Denial of Service through Malformed Inputs	7.5	Medium
Home Assistant Hub	CVE-2023-5007	Eavesdropping vulnerability in voice commands	8.2	High
NAS Server	CVE-2023-5008	SQL injection in device management interface	9.0	High

Result

Effectiveness of deception

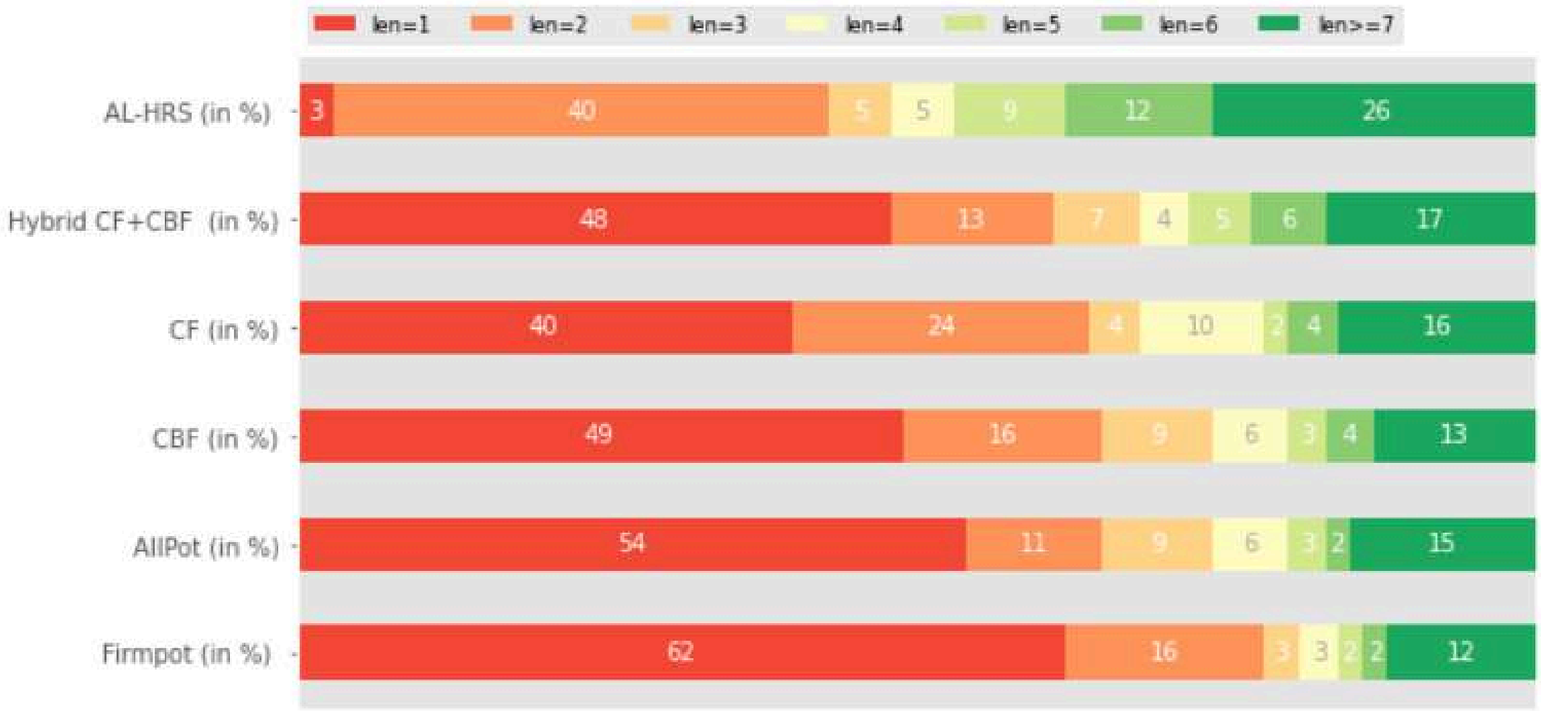


Table 4 – *Comparison of targeting metrics in deception system.*

Method	Total number of requests received / total number of request targeting recommended vulnerabilities
AL-HRS	9,235 / 5,287
Hybrid CF+CBF	7,235 / 1,917
CF only	6,235 / 1,087
CBF only	5,235 / 993
AIIPot (5)	6,235 / 987
Firmpot (98)	2,896 / 687

Figure 9 – Comparison of attacker engagement times with recommended vulnerabilities by AL-HRS and existing method.

Result

Effectiveness of deception

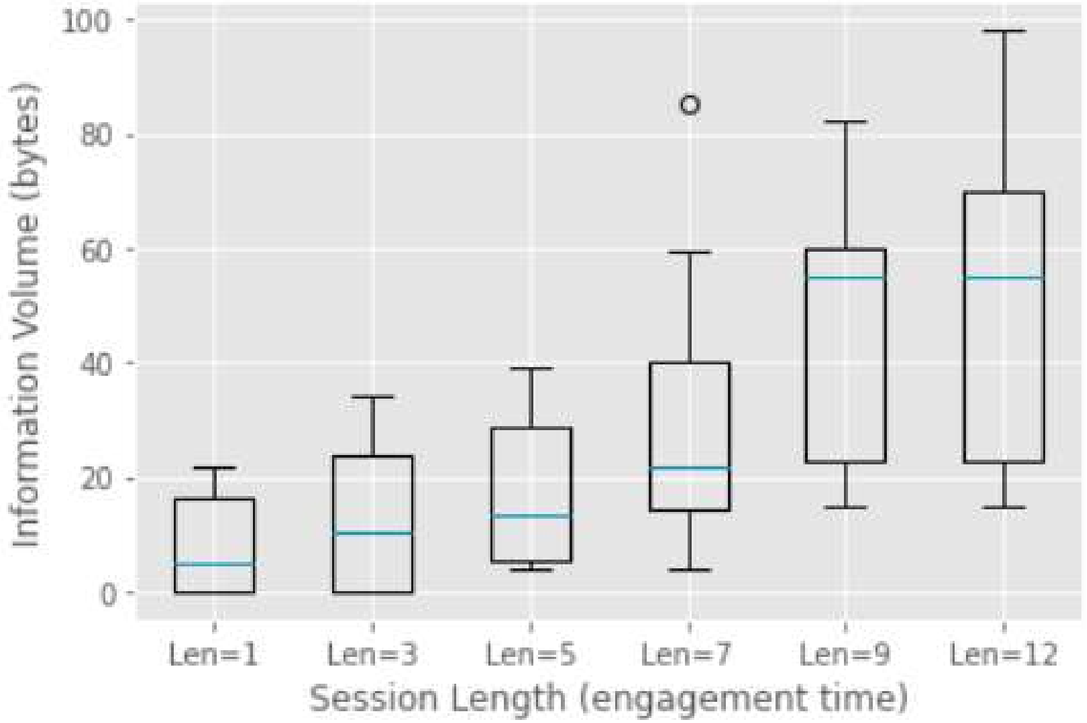


Figure 10: Correlation between engagement time and volume of information sent by attackers

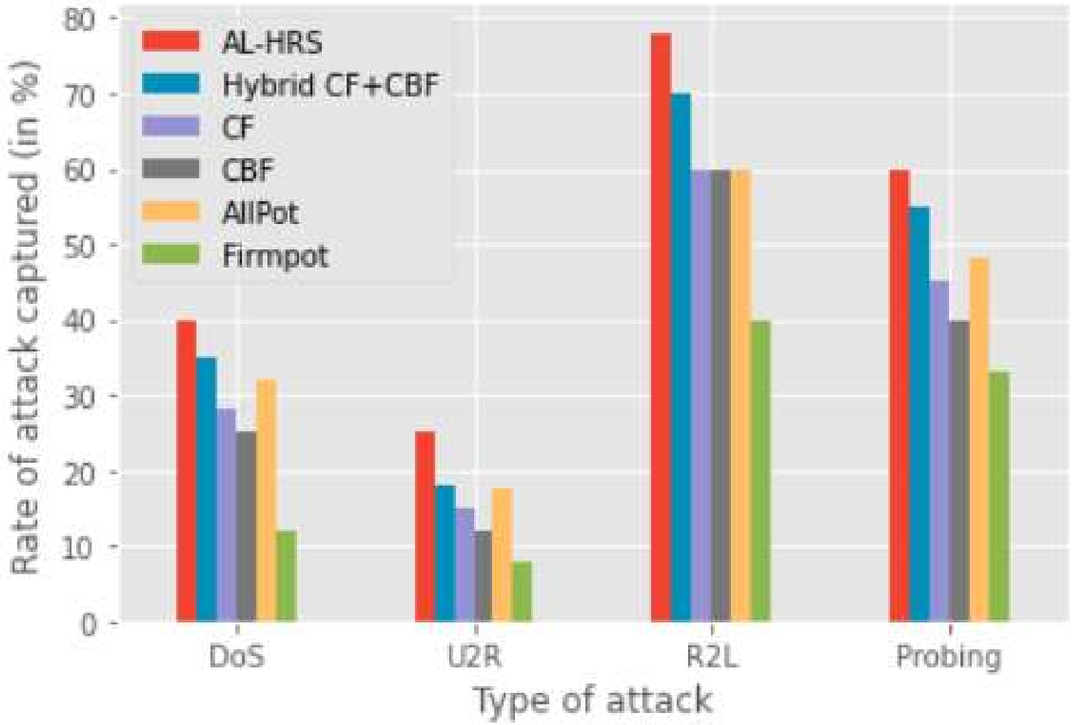
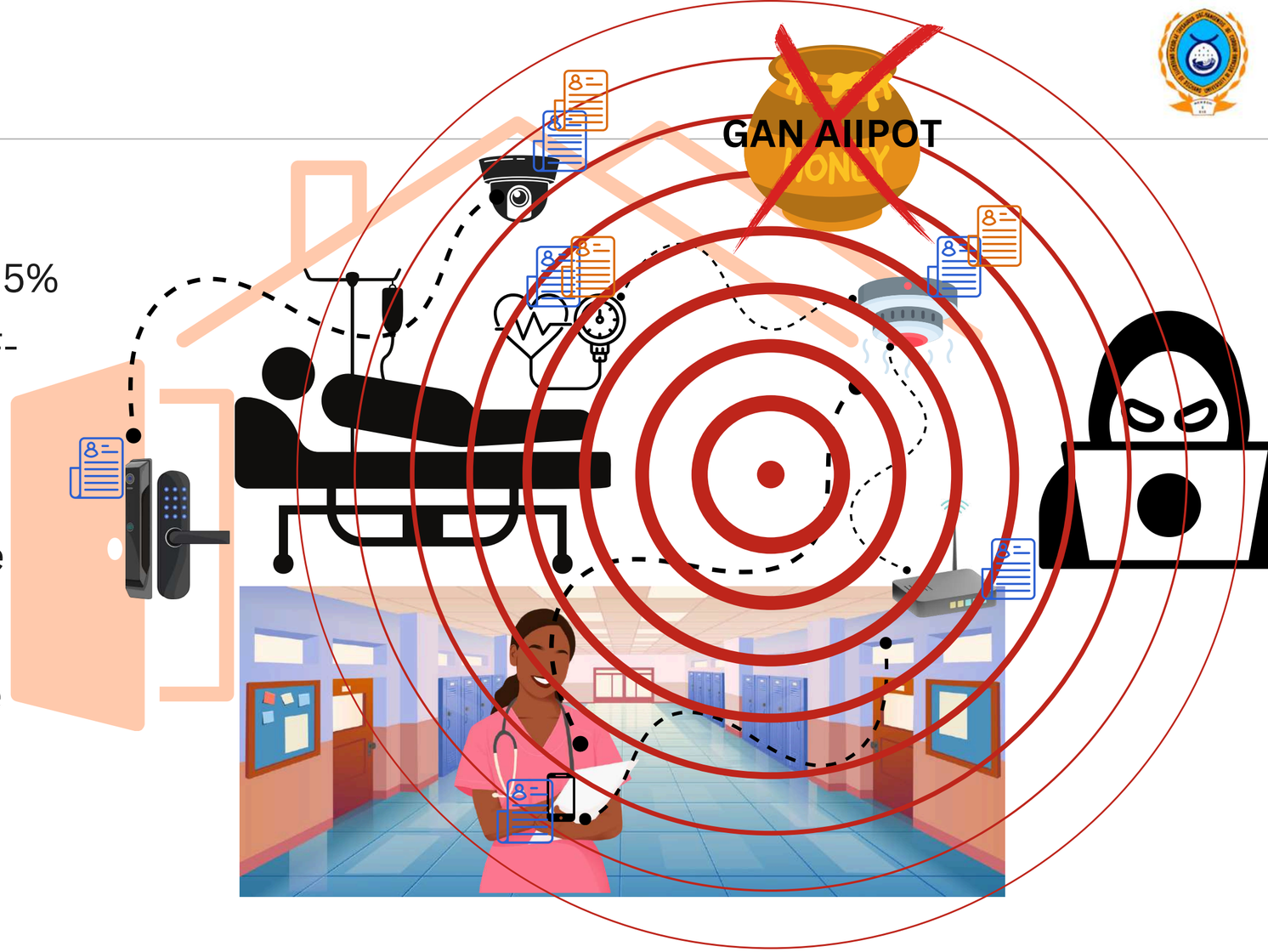


Figure 11: Detection rate of AL-HRS

Analysis & Discussion

- **High Accuracy:**
  - Precision: 92%, Recall: 89%, F1 Score: 90.5%
  - Outperforms traditional CF-only and CBF-only method**s.**
- **Effective Deception:**
  - Engages 26% of attackers with a 7-minute average session duration.
  - Longer engagements correlate with more detailed intelligence gathering.
- **Scalability & Efficiency:**
  - Maintains sub-2-second response time in 95% of cases, even with 100 devices.
  - Successfully mitigated over 50% of advanced threats.



Contribution 3

Advanced Security using Augmented Reality Honeypots: A Case Study for IoT Cameras

V.S Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack and C. Kamhoua, "ARPotCam: Augmented Reality-Driven Honeypot for Enhancing Security in IoT Surveillance Systems,'' The Visual Computer, Springer

IoT cameras are being deployed everywhere

IoT Cameras

Smart City

Home Security

Military Operation

Drone

Motivation

The security challenge for IoT camera-based systems need to be addressed

Bloomberg

Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

LILY HAY NEWMAN SECURITY NEWS AUG 17, 2021 8:00 AM

Millions of Web Camera and Baby Monitor Feeds Are Exposed

CNN BUSINESS Markets Tech Media Success Perspectives Videos LIVE TV Edition

Companies on alert after apparent hack of cloud-based security camera service

By Brian Fung, CNN Business

Updated 4:32 PM ET, Wed March 10, 2021

Motivation

Honeypot can help!

- It can inform the defender that an attack is ongoing
- It can help the defender learn attack behavior
- It can engage the attacker and waste their time/resource
- It can even deceive the attacker with falsely information and affect their decision-making process

Home surveillance:

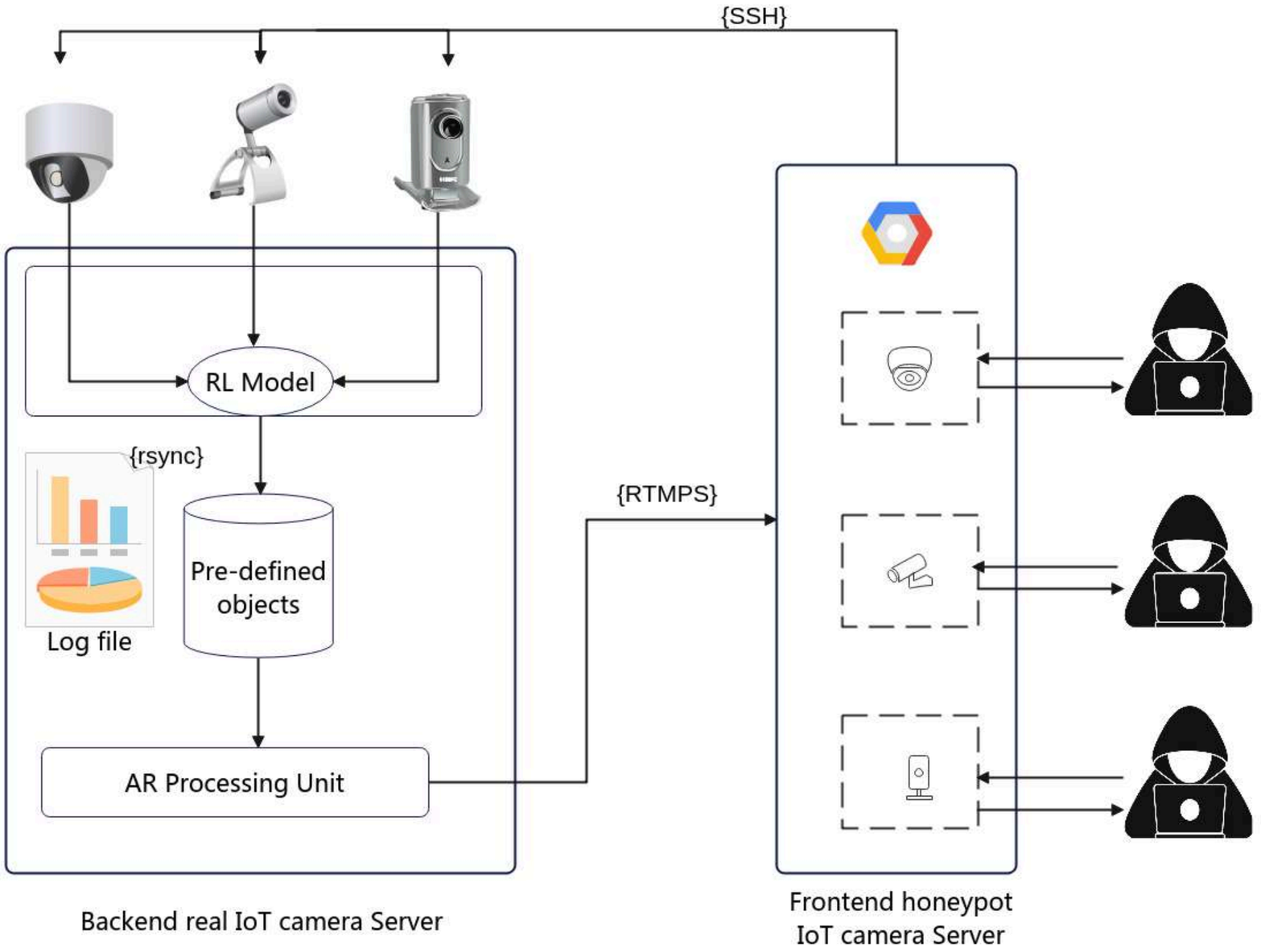
- A thief may compromise surveillance cameras to check if anyone is at home, and then perform a real-life attack (stealing Amazon packages, etc).
- Deception: show cars parking in the garage.

Military:

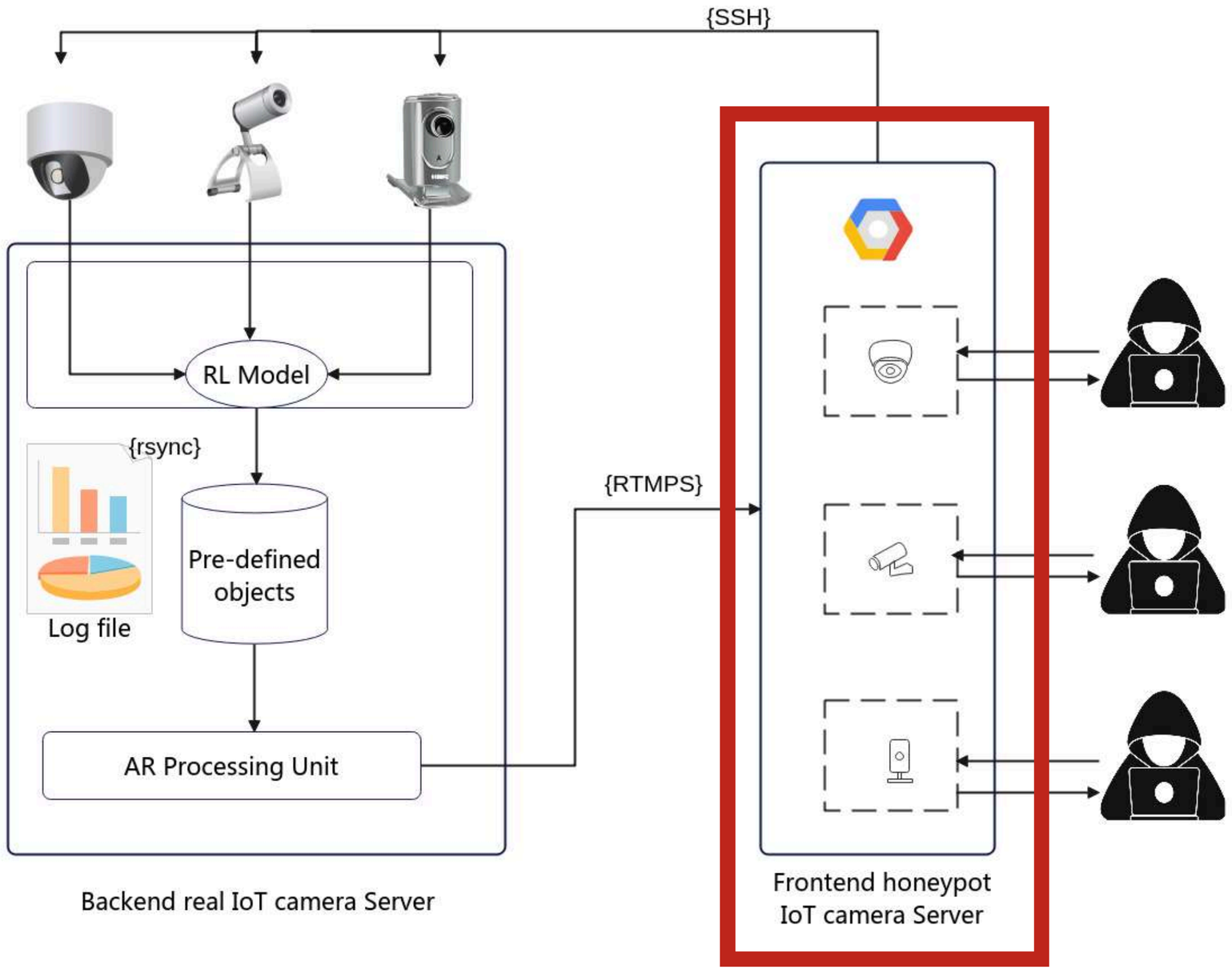
- Compromise soldier-mounted cameras or drone cameras to obtain tactical and battlefield information.
- Deception: The honeypot shows troops moving left, but actually moving right.

Threat Model

System Overview



Frontend Honeypot



Frontend Honeypot

- **Realistic Interaction**:

Emulates critical services and ports (e.g., Port 80/8080 for the web interface, Port 8000 for ONVIF, Port 554 for RTSP) to appear as a genuine IoT camera, effectively engaging attackers.

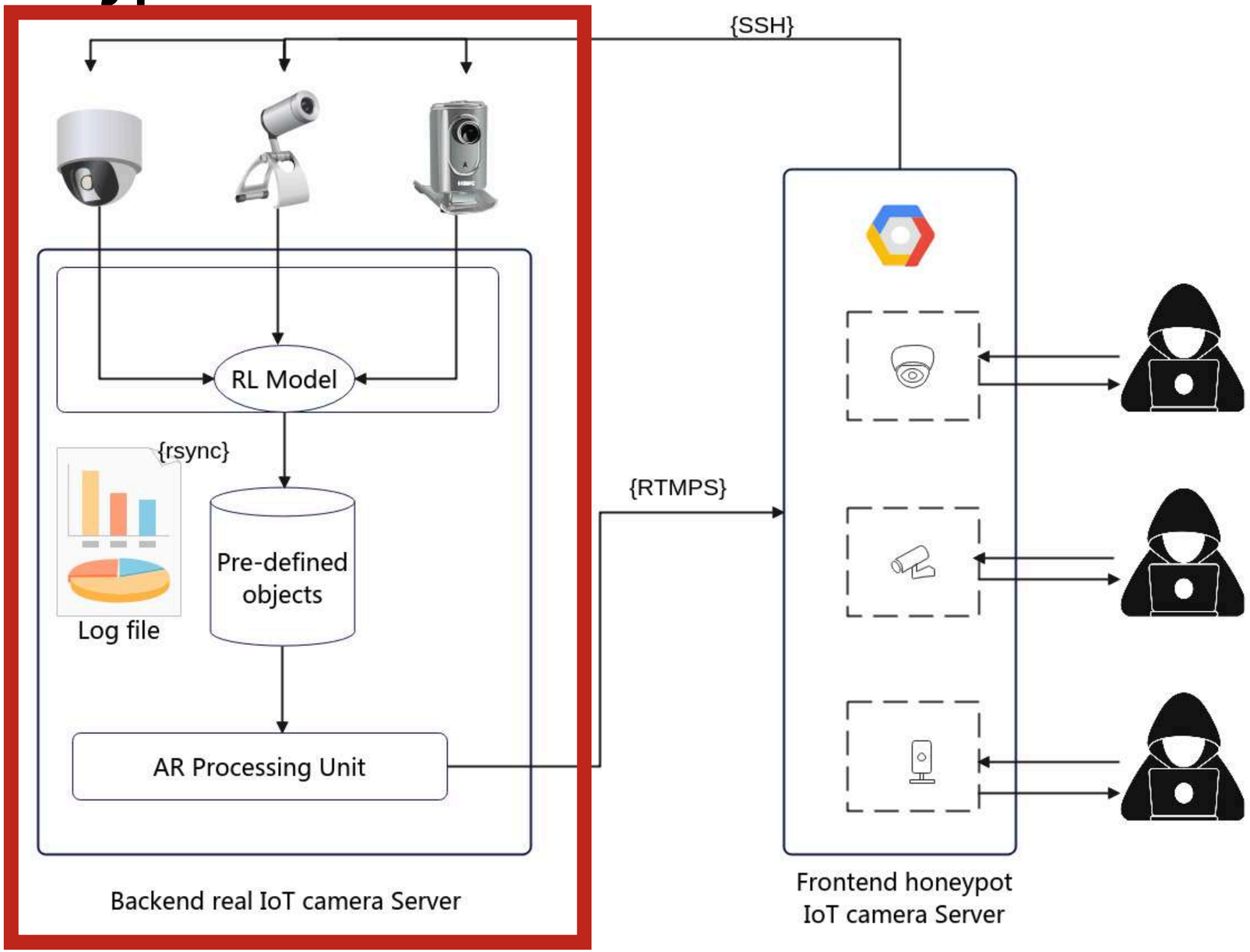
- **Seamless Deception:**

Forwards attacker commands to a backend real IoT camera, with augmented video streams relayed back to the attacker, ensuring the integrity of the deception.

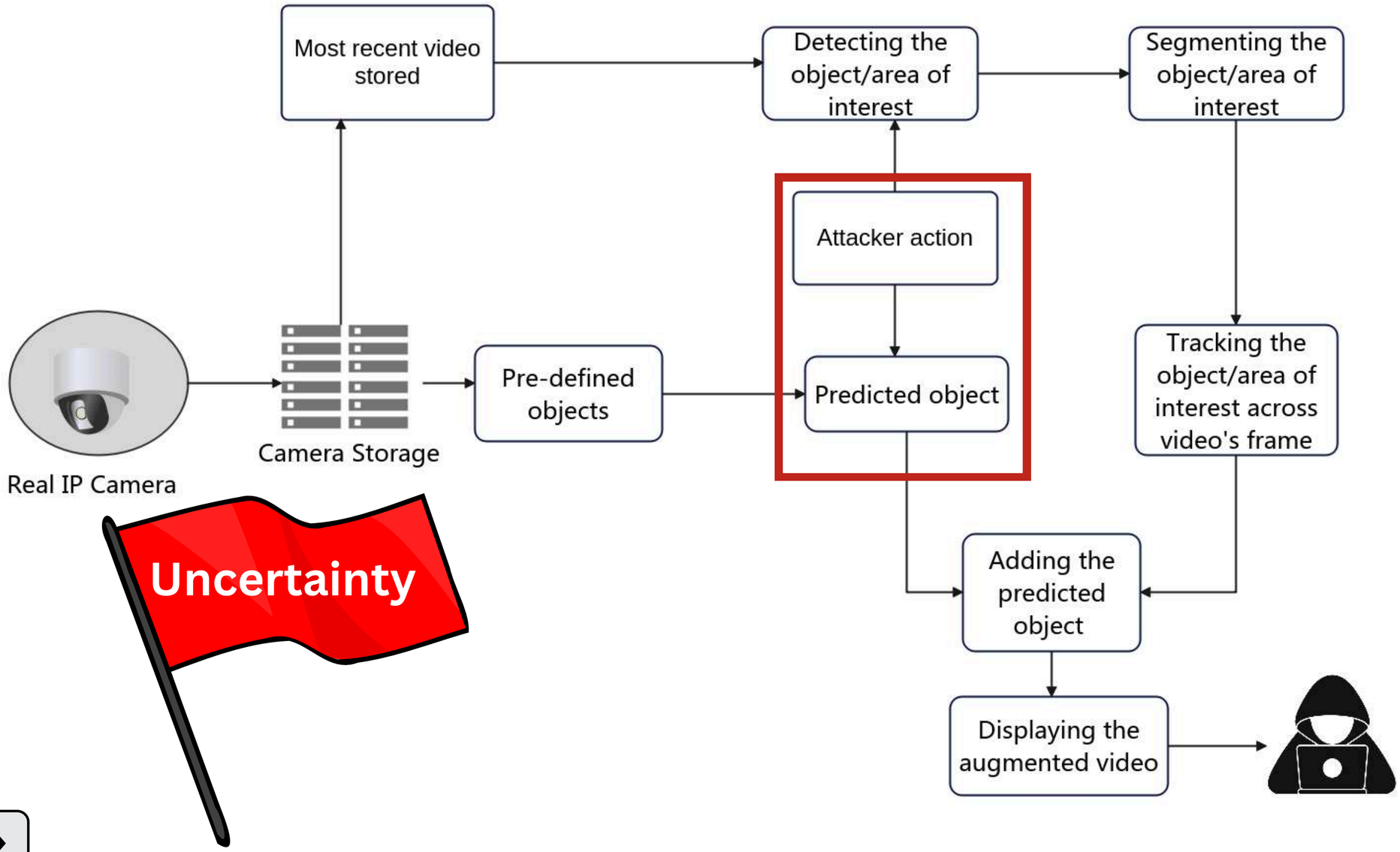
- **Scalable Deployment:**

Operates as a lightweight server, enabling easy deployment of multiple honeypots on cloud platforms with minimal computational resources.

Backend Honeypot



AR Processing Unit



Dynamic BehavioR Emulation

- RL dynamically adapts camera responses based on attacker actions, e.g., adjusting objects in the view to match attacker interests.

- Q-learning is used to train the RL agent in a simulated environment, optimizing deception strategies by adjusting Q-values for state-action pairs.

- Q-learning helps the system learn the best actions to take in response to attacker behavior by updating a Q-value for each possible action

Dynamic Behavior Emulation

- **Key RL Elements:**
  - States (a): Camera view angles, augmented objects, security settings.
  - Actions (s): Adjusting camera views, adding/removing objects, altering settings.
  - Rewards (r): Positive for successful deception, and longer interaction times; negative for detection.
  - Transition Probabilities: Influence of actions on the likelihood of continued attacker engagement.
- **Q-Value Q(s,a):**
  - The value represents the expected future reward of taking action aaa in state
  - Updated through experience as the system learns which actions are most effective.
  - Goal: Maximize Q(s,a) to predict the best action for maintaining deception.

Dynamic Behavior Emulation

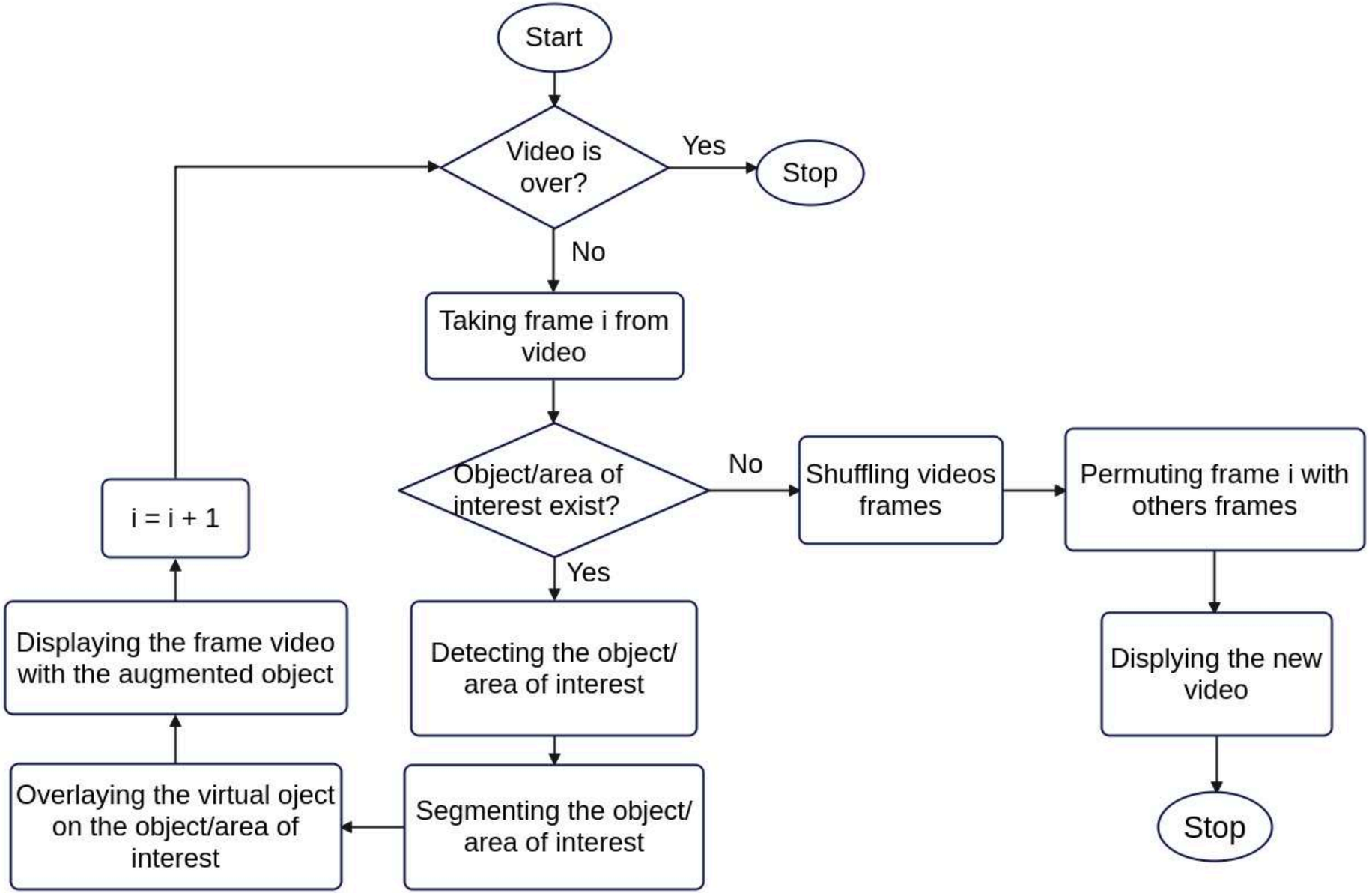
- **Update:** The Q-value is updated using the formula:

$$Q(s,a) \leftarrow Q(s,a) + \alpha \left[r + \gamma \max_{a'} Q(s',a') - Q(s,a) \right]$$

  - $Q(s,a)$: Current estimate of how good the action a is in state s.
  - r: Immediate reward received after taking action a.
  - γ: Discount factor balancing immediate and future rewards.
  - $\max_{a'} Q(s',a')$: Best possible future reward from next state s'.

$$\text{MSE} = \frac{1}{N} \sum_{i=1}^{N} \left(Q(s_i,a_i) - \left[r_i + \gamma \max_{a'} Q(s_i',a') \right] \right)^2,$$

AR processing unit



Implementation

CONFIGURING VIDEO STREAMS

Real IoT camera captures live video, which is forwarded to the AR processing unit. Virtual servers for frontend honeypot IoT cameras are configured to receive augmented streams, with necessary ports opened for streaming protocols (RTSP, RTMP) and interactive controls.

CREATION OF AR ENVIRONMENT

Developed using Unity3D and ARCore, with augmented objects dynamically added based on RL model predictions of attacker behavior, enhancing the deception by aligning with attacker interests.

COMMUNICATION AND INTERACTION

Frontend honeypot cameras send attacker commands to the backend IoT camera via secure SSH connections, with all interactions logged and processed to maintain confidentiality and gather intelligence.

Comparisons:

- Real-Camera: A real-camera-based honeypot. It also provides camera control functionality
- Recorded video: A low-interaction camera honeypot based on recorded video. It does not provide camera control functionality
- HoneyCam

Result

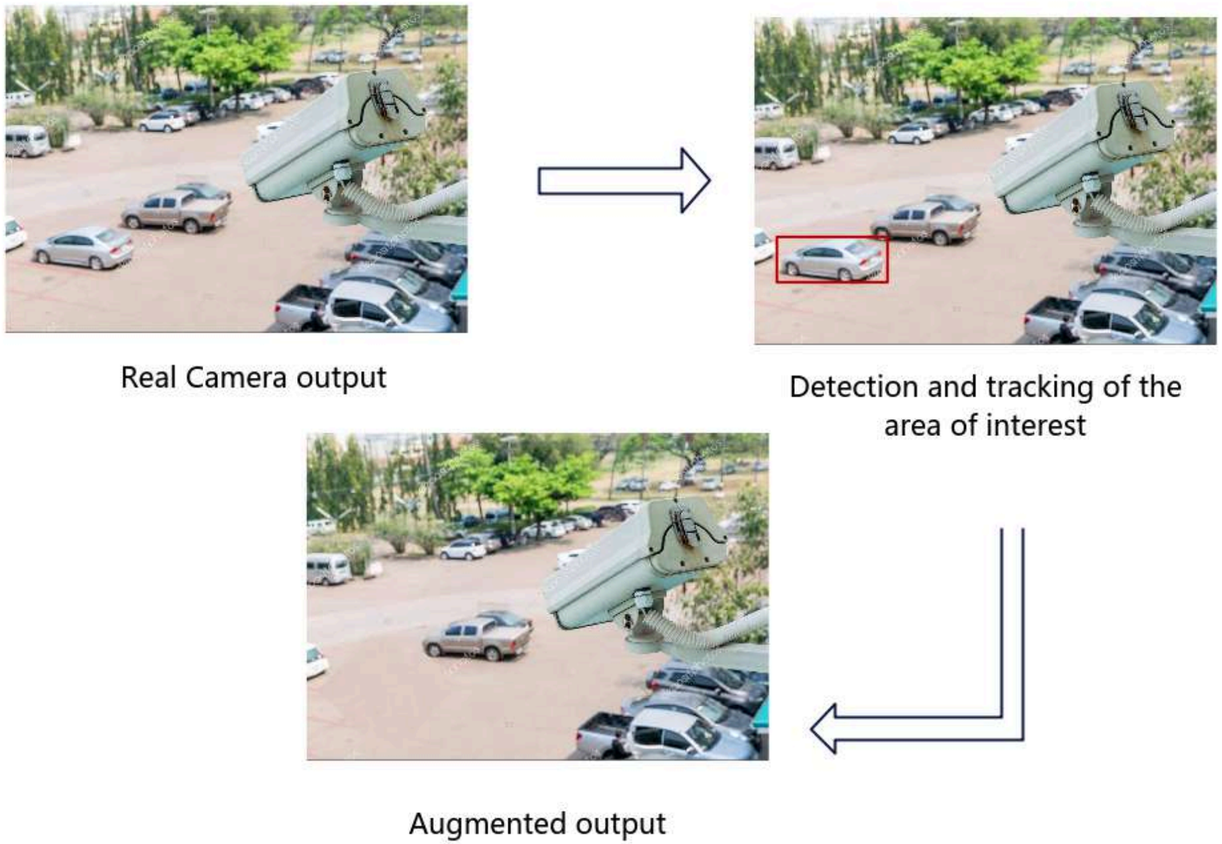


Figure 12 – Example of AR video frame.

Method	Total number of distinct remote
ARPotCam	**27869**
HoneyCam (7)	24120
Real-Camera-Honeypot (6)	26770
Recorded Video Stream (102)	25770

Table 5 – Number of requests received by each honeypot on the GCP web server

Result

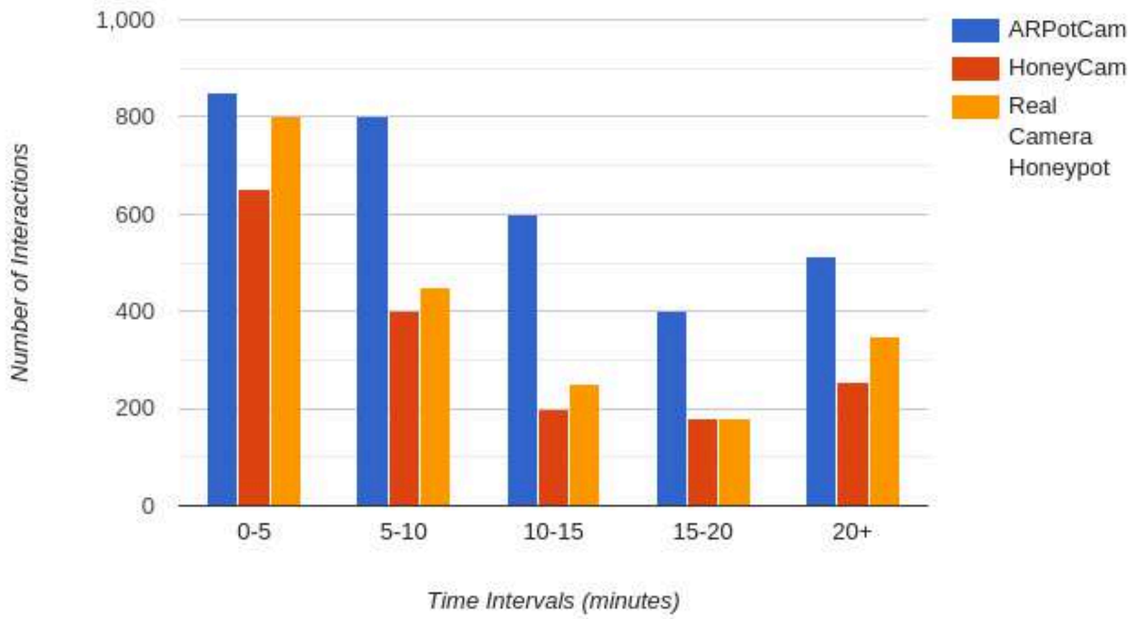


Figure 13– Duration an attacker spends interacting with the honeypot.

Method	Port scan attacks	Attackers access the video stream	Attackers interact with camera command
ARPotCam	25100	2674	2012
HoneyCam (7)	24120	1608	1336
Real Camera Honeypot (6)	23658	1534	1032
Recorded Video Stream (102)	23570	1034	0

Table 5 – Types of attack interactions captured

Result

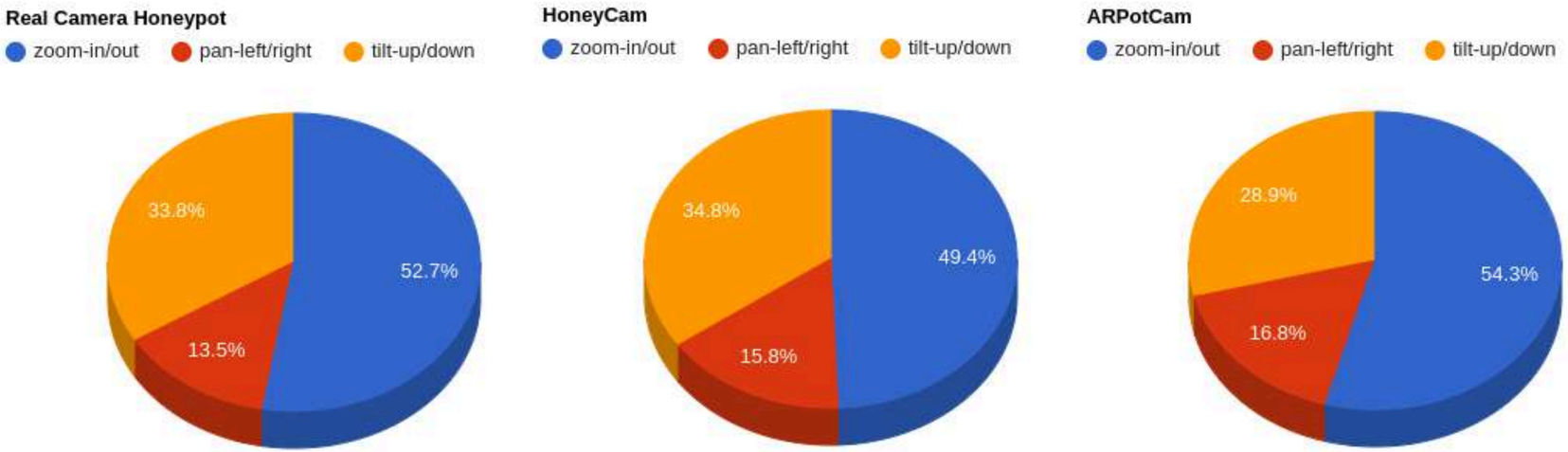


Figure 14 – Varieties of camera control command distribution. (a) Real-Camera Honeypot (6), (b) HoneyCam (7), (c) ARPotCam

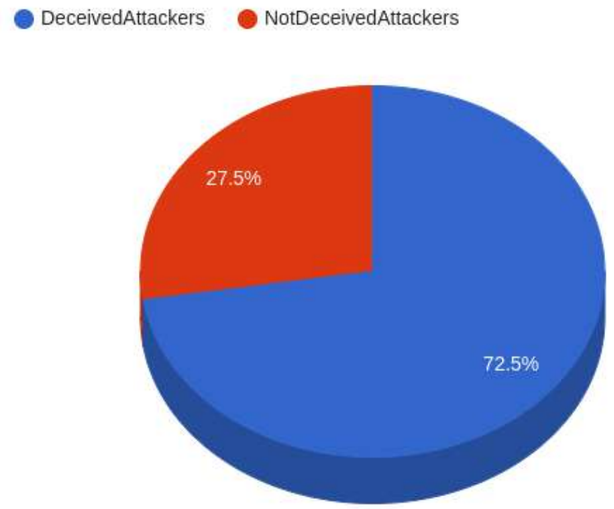


Figure 15 – Proportion of attackers misled by the honeypot.

Result

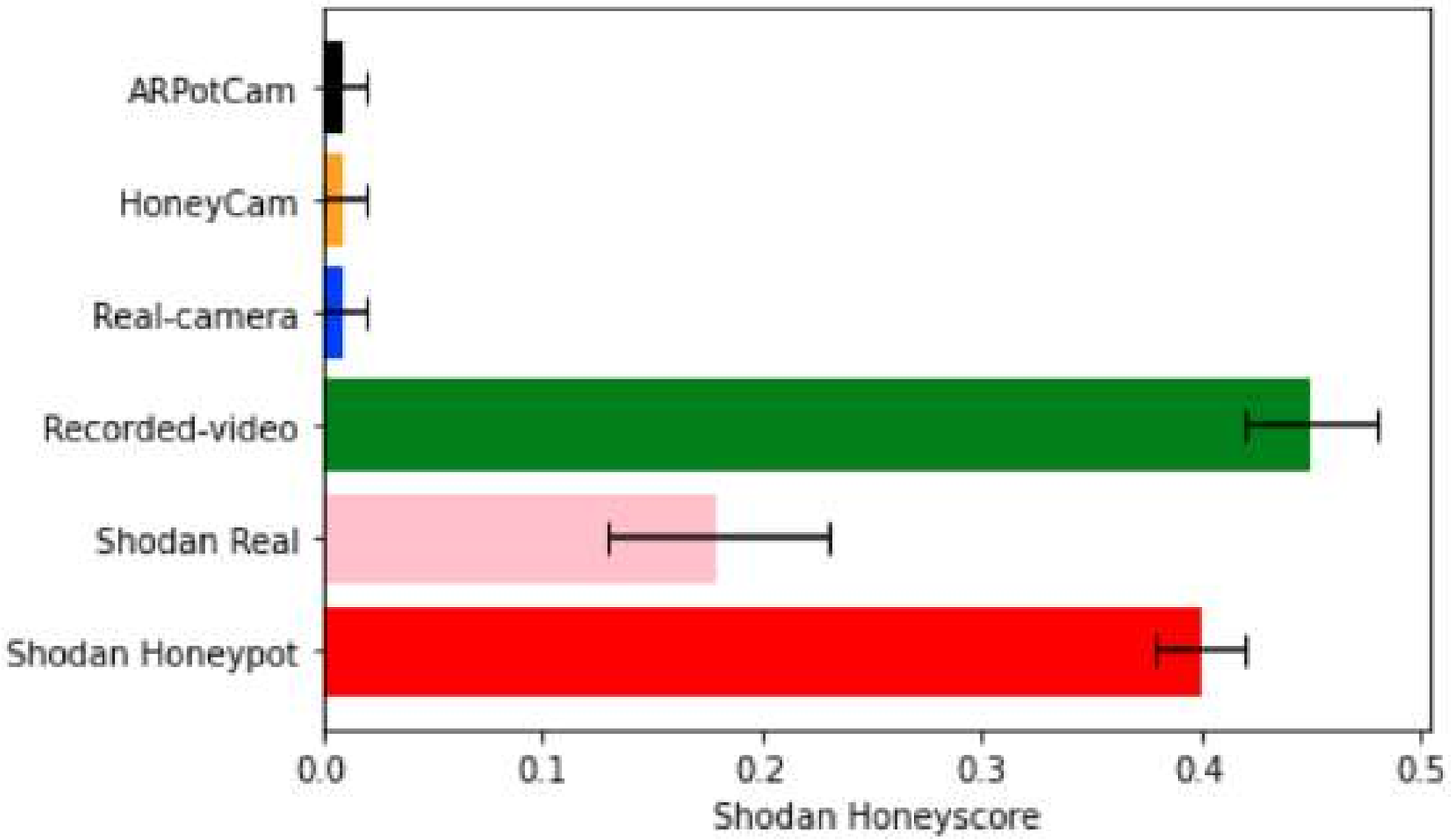


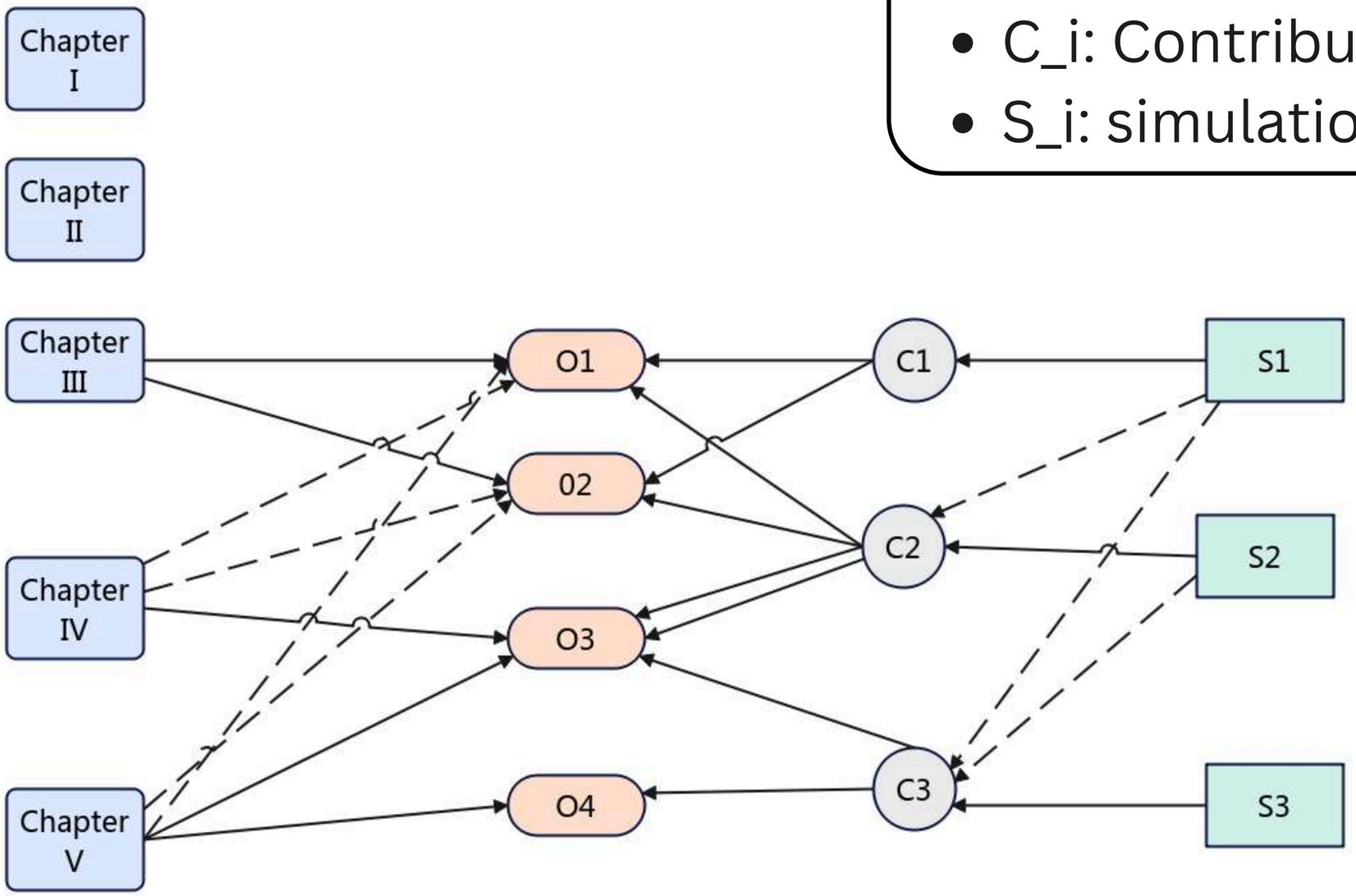
Figure 16 – Covertness Evaluation: Percentage of Attackers Deceived

Analysis & Discussions

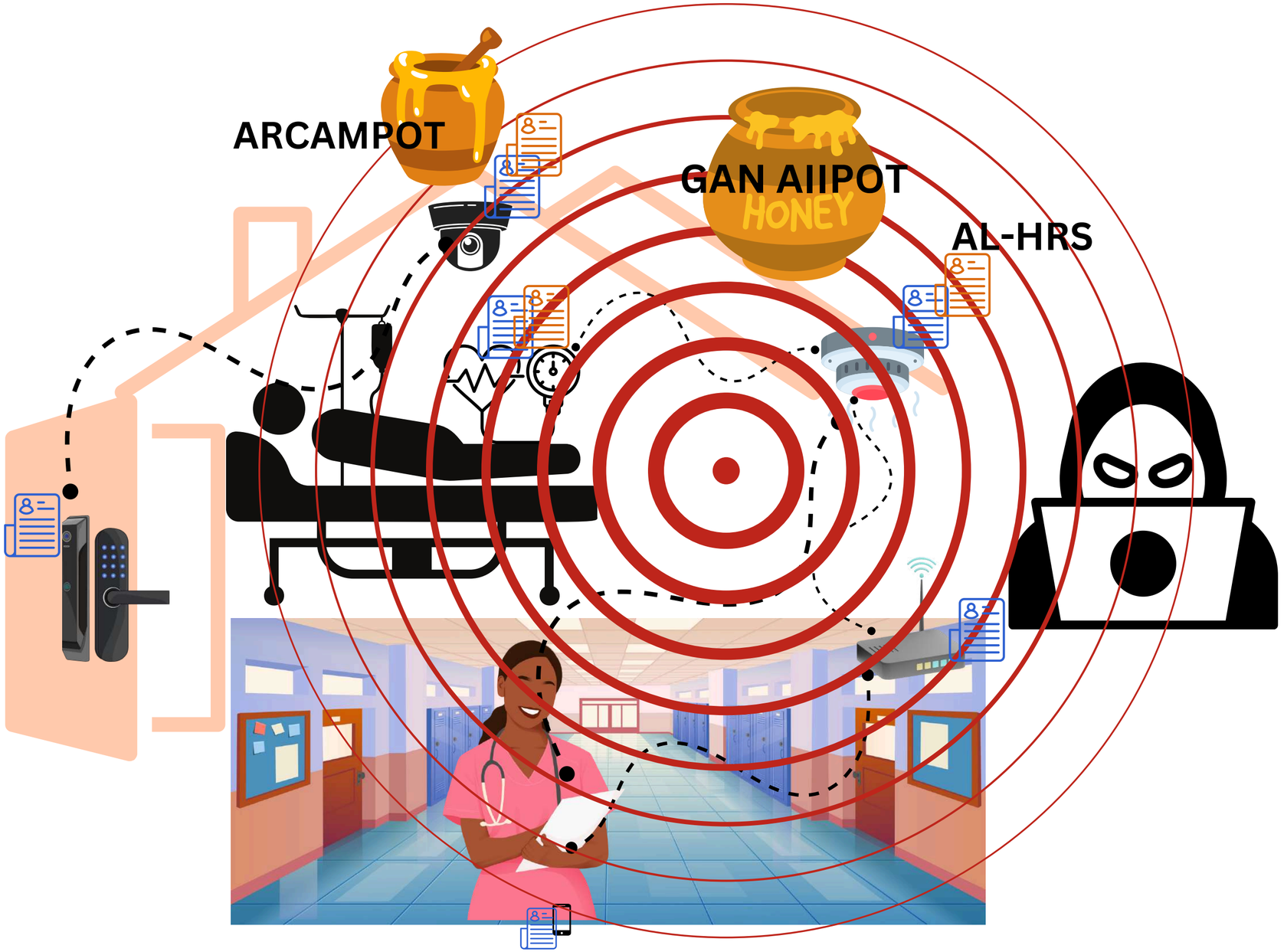
- **High Engagement & Deception:**
  - 27,869 attacker connections with a 72.5% deception rate.
  - Longer attacker engagement times, enhanced by realistic video interactions (zoom, tilt, pan).
- **Adaptive & Scalable:**
  - Uses RL to tailor deception tactics in real-time, adapting based on attacker behavior.
  - Successfully handles the increased load with no performance degradation; low latency (150ms avg, 200ms max).

Summary

- 0_i: Specific objective
- C_i: Contribution
- S_i: simulation



Summary



Future works

Advanced ML Integration:

- Explore deep learning and ensemble methods for improved detection accuracy and adaptability.
- Enhance robustness and performance in IoT security solutions.

Comprehensive Datasets:

- Develop broader datasets capturing diverse IoT behaviors and attack vectors.
- Improve the generalizability and effectiveness of ML models in real-world environments.

Scalability:

- Investigate the deployment of security systems in large-scale IoT ecosystems.
- Optimize computational resources and ensure real-time threat detection.

Ethical Considerations:

- Examine the ethical implications of using cyber deception in IoT security.
- Develop guidelines balancing security needs with ethical and legal concerns.

Sector-Specific Recommendations

Sector	Action Plan	Impact	Challenges	Timeline
Defense	Deploy intelligent honeypots in sensitive sites	Early threat detection & reduced intrusions	High cost, expertise needed	6-18 months
Healthcare	Secure medical IoT devices	Patient data protection & system resilience	Regulatory compliance	3-12 months
Finance	Strengthen banking & ATM security	Fraud prevention & customer trust	Legacy system integration	6-18 months
Transport	Enhance security in smart transport networks	Safer public transport & real-time threat monitoring	Managing real-time responses	9-24 months

Refences 1/2

List of Publications

1. V. S. Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack and C. Kamhoua, "Adaptive Learning-Based Hybrid Recommender System for Deception in Internet of Thing, " Computer Networks, Volume 255, 2024, 110853, ISSN 1389 1286, doi:10.1016/j.comnet.2024.110853
2. Volviane Saphir Mfogo, Alain Zemkoho, Laurent Njilla, Marcellin Nkenlifack, and Charles Kamhoua. Aiipot: Adaptive intelligent-interaction honeypot for IoT devices. In 2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, Toronto, ON, Canada, 2023, pp. 1-6, doi:10.1109/PIMRC56721.2023.10293827
3. V. S. Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack and C. Kamhoua, ‘’Deceptive Approach for Internet of Things Security with Machine Learning. In 2024 IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things, IEEE, Mt. Pleasant, Michigan, USA, 2024, pp. 1-5, doi: 10.1109/AIBThings63359.2024.10863491

Refences 2/2

List of Publications (Accepted & Under Review)

- V. S. Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack and C. Kamhoua, "ARPotCam: Augmented Reality-Driven Honeypot for Enhancing Security in IoT Surveillance Systems" The Visual Computer, Springer, doi:10.1007/s00371-025-03880-2.

- V. S. Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack and C. Kamhoua, "GAN-AIIPot: GAN-based Cyber Deception for Probing Attacks on IoT Devices." IEEE Transactions on Network and Service Management, **February 2025, Major Revision**.

Acknowledgments

Research team

Prof Marcellin Nkenlifack
Full Professor
Department of Mathematics & Computer Science
University of Dschang

Prof Alain Zemkoho
Full Professor
School of Mathematical Sciences
University of Southampton

Dr Laurent Njilla
Senior Research Engineer
Information Assurance Branch
Air Force Research Laboratory

Dr Charles Kamhoa
Senior Research Engineer
Network Security Branch
DEVCOM Army Research Laboratory
Adelphi, MD, USA

Sponsors

DEVCOM ARMY RESEARCH LABORATORY

Project GMC-DRA

THANK YOU
for Listening

QUESTIONS?

Feel safe with your IoT device!!!